



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10013808 A**

(43) Date of publication of application: **16.01.98**

(51) Int. Cl

H04N 7/16

(21) Application number: 08163284

(22) Date of filing: **24.06.96**

(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**

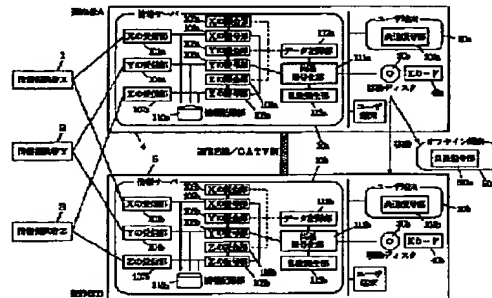
(72) Inventor: OMORI MOTOJI
MATSUZAKI NATSUME
TATEBAYASHI MAKOTO

(54) INFORMATION SERVICE SYSTEM

(57) Abstract:

PROBLEM TO BE SOLVED: To provide an information service system by which the information served by the service provider is charged on a contractor depending on the degree of use when the contractor records the information and uses it repetitively.

SOLUTION: An information server adds charge reference data to information to be served and distributes the resulting information. A contractor A4 is provided with an information server 10a and a user terminal equipment 20a, and a reception section 1101a of an X information server 10a receives information distributed by the information server X1. An information reception section 110a records the information received by the X reception section 101a. An X imposing section 103a calculates the charge of the information based on charging basis data added to the information every time the information recorded by the information recording section 110 is sent to the user terminal equipment 20a. A data recording display section 112a records the utility charge calculated and obtained by the X charging section 103a.



COPYRIGHT: (C)1998,JPO

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-13808

(43)公開日 平成10年(1998) 1月16日

(51)Int.Cl.⁶
H 0 4 N 7/16

識別記号 庁内整理番号

F I
H 0 4 N 7/16

技術表示箇所

C

審査請求 未請求 請求項の数102 O L (全 39 頁)

(21)出願番号 特願平8-163284

(22)出願日 平成8年(1996) 6月24日

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 大森 基司

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 松崎 なつめ

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 館林 誠

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

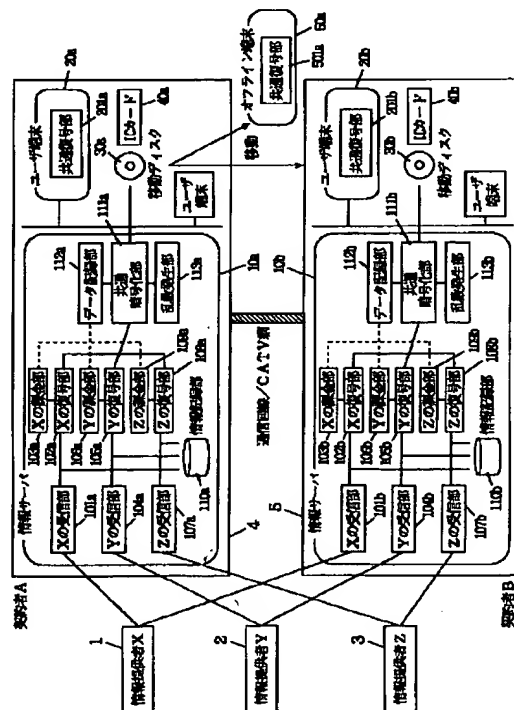
(74)代理人 弁理士 小笠原 史朗

(54)【発明の名称】 情報提供システム

(57)【要約】

【課題】 情報提供者が提供する情報を、契約者が記録して繰り返し利用する場合、利用度合に応じて課金することができる情報提供システムを提供する。

【解決手段】 情報提供者X 1は、提供すべき情報に、課金基準データを付加して配信する。契約者A 4には、情報サーバ10aおよびユーザ端末20aが設けられており、情報サーバ10aのXの受信部101aは、情報提供者X 1が配信する情報を受信する。情報記録部110aは、Xの受信部101aが受信した情報を記録する。Xの課金部103aは、情報記録部110aに記録された情報が、ユーザ端末20aに伝達される毎に、その情報に付加された課金基準データに基づいて、その情報の利用料金を算定する。データ記録部112aは、Xの課金部103aが算定して得られた利用料金を記録する。



【特許請求の範囲】

【請求項 1】 1 以上の情報提供者と契約者とは、
 情報提供者は、契約者に情報を提供し、契約者は、
 提供される情報を利用して、情報提供者に利用料金を支
 払うような情報提供システムであって、
 前記 1 以上の情報提供者側にはそれぞれ、提供すべき情
 報に、当該情報の利用料金を算定するための課金基準デ
 ータを付加して配信する配信手段が設けられ、
 前記契約者側には、情報サーバおよび当該情報サーバに
 情報伝達可能に接続された 1 以上の端末が設けられ、
 前記情報サーバは、
 前記 1 以上の情報提供者が提供する情報を受信する受信
 手段と、
 前記受信手段が受信した情報を記録する情報記録手段
 と、
 前記情報記録手段が記録した情報が、前記 1 以上の端末
 に伝達される毎に、当該情報に付加されている課金基準
 データに基づいて、当該情報の利用料金を算定する課金
 手段と、
 前記課金手段が算定して得られた利用料金を記録するデ
 ータ記録手段とを備える情報提供システム。

【請求項 2】 前記 1 以上の情報提供者が提供する情報
 は、それぞれ暗号化されており、
 前記情報サーバは、前記情報記録手段が記録した情報を
 復号する第 1 の復号手段をさらに備えることを特徴とす
 る、請求項 1 に記載の情報提供システム。

【請求項 3】 前記データ記録手段は、前記 1 以上の端
 末毎の秘密鍵を記憶しており、
 前記情報サーバは、前記第 1 の復号手段が復号して得ら
 れた情報を、前記データ記録手段が記憶している前記 1
 以上の端末毎の秘密鍵でそれぞれ再暗号化する共通暗号
 化手段をさらに備え、
 前記 1 以上の端末はそれぞれ、自己の秘密鍵を記憶して
 おり、前記情報サーバから伝達された、再暗号化された
 情報を、当該秘密鍵で復号する第 2 の復号手段を備える
 ことを特徴とする、請求項 2 に記載の情報提供システ
 ム。

【請求項 4】 前記データ記録手段は、前記 1 以上の端
 末毎の秘密鍵を記憶しており、
 前記情報サーバは、
 乱数を発生する乱数発生手段と、
 前記第 1 の復号手段が復号して得られた情報を、前記乱
 数発生手段が発生する乱数で再暗号化し、かつ、当該乱
 数を、前記データ記録手段が記憶している前記 1 以上の
 端末毎の秘密鍵でそれぞれ暗号化する共通暗号化手段と
 をさらに備え、
 前記 1 以上の端末はそれぞれ、自己の秘密鍵を記憶して
 おり、前記情報サーバから伝達された、暗号化された乱
 数を、当該秘密鍵で復号し、かつ前記情報サーバから伝
 達された、再暗号化された情報を、復号して得た乱数で

復号する第 2 の復号手段を備えることを特徴とする、請
 求項 2 に記載の情報提供システム。

【請求項 5】 1 以上の情報提供者と契約者とは、
 情報提供者は、契約者に情報を提供し、契約者は、
 提供される情報を利用して、情報提供者に利用料金を支
 払うような情報提供システムの契約者側に設けられる情
 報サーバであって、
 前記 1 以上の情報提供者はそれぞれ、提供すべき情報
 に、当該情報の利用料金を算定するための課金基準デー
 タを付加して配信し、
 前記契約者側には、さらに、当該情報サーバに情報伝達
 可能に接続された 1 以上の端末が設けられており、
 前記 1 以上の情報提供者が提供する情報を受信する受信
 手段と、
 前記受信手段が受信した情報を記録する情報記録手段
 と、
 前記情報記録手段が記録した情報が、前記 1 以上の端末
 に伝達される毎に、当該情報に付加されている課金基準
 データに基づいて、当該情報の利用料金を算定する課金
 手段と、
 前記課金手段が算定して得られた利用料金を記録するデ
 ータ記録手段とを備える情報サーバ。

【請求項 6】 前記 1 以上の情報提供者が提供する情報
 は、それぞれ暗号化されており、
 前記情報記録手段が記録した情報を復号する復号手段を
 さらに備えることを特徴とする、請求項 5 に記載の情報
 サーバ。

【請求項 7】 前記 1 以上の端末はそれぞれ、自己の秘
 密鍵を記憶しており、前記情報サーバから伝達された、
 再暗号化された情報を、当該秘密鍵で復号する機能を有
 し、
 前記データ記録手段は、前記 1 以上の端末毎の秘密鍵を
 記憶しており、
 前記復号手段が復号して得られた情報を、前記データ記
 録手段が記憶している前記 1 以上の端末毎の秘密鍵でそ
 れぞれ再暗号化する共通暗号化手段をさらに備えること
 を特徴とする、請求項 6 に記載の情報サーバ。

【請求項 8】 前記 1 以上の端末はそれぞれ、自己の秘
 密鍵を記憶しており、前記情報サーバから伝達された、
 暗号化された乱数を、当該秘密鍵で復号し、かつ、前記
 情報サーバから伝達された、再暗号化された情報を、復
 号して得た乱数で復号する機能を有し、
 前記データ記録手段は、前記 1 以上の端末毎の秘密鍵を
 記憶しており、
 乱数を発生する乱数発生手段と、
 前記復号手段が復号して得られた情報を、前記乱数発生
 手段が発生する乱数で再暗号化し、かつ、当該乱数を、
 前記データ記録手段が記憶している前記 1 以上の端末毎
 の秘密鍵で暗号化する共通暗号化手段とをさらに備える
 ことを特徴とする、請求項 6 に記載の情報サーバ。

【請求項 9】 1 以上の情報提供者と契約者とからなり、情報提供者は、契約者に情報を提供し、契約者は、提供される情報を利用して、情報提供者に利用料金を支払うような情報提供システムの契約者側に設けられる端末であって、

前記 1 以上の情報提供者はそれぞれ、提供すべき情報を暗号化したうえ、当該情報の利用料金を算定するための課金基準データを付加して配信し、

前記契約者側には、前記端末の秘密鍵を記憶しており、前記 1 以上の情報提供者が提供する情報を受信し、かつ受信した情報を記録し、かつ記録した情報が前記端末に伝達される毎に、当該情報に付加されている課金基準データに基づいて当該情報の利用料金を算定し、かつ算定して得た利用料金を記録し、かつ記録した情報を復号し、かつ復号して得た情報を当該秘密鍵で再暗号化する機能を有する情報サーバがさらに設けられ、

自己の秘密鍵を記憶しており、前記情報サーバから伝達された、再暗号化された情報を、当該秘密鍵で復号する復号手段を備える端末。

【請求項 10】 1 以上の情報提供者と契約者とからなり、情報提供者は、契約者に情報を提供し、契約者は、提供される情報を利用して、情報提供者に利用料金を支払うような情報提供システムの契約者側に設けられる端末であって、

前記 1 以上の情報提供者はそれぞれ、提供すべき情報を暗号化したうえ、当該情報の利用料金を算定するための課金基準データを付加して配信し、

前記契約者側には、前記端末の秘密鍵を記憶しており、前記 1 以上の情報提供者が提供する情報を受信し、かつ受信した情報を記録し、かつ記録した情報が前記端末に伝達される毎に、当該情報に付加されている課金基準データに基づいて当該情報の利用料金を算定し、かつ算定して得た利用料金を記録し、かつ記録した情報を復号し、かつ乱数を発生し、かつ復号して得た情報を当該乱数で再暗号化し、かつ当該乱数を当該秘密鍵で暗号化する機能を有する情報サーバがさらに設けられ、

自己の秘密鍵を記憶しており、前記情報サーバから伝達された、暗号化された乱数を、当該秘密鍵で復号し、かつ前記情報サーバから伝達された、再暗号化された情報を、復号して得た乱数で復号する復号手段を備える端末。

【請求項 11】 1 以上の情報提供者と契約者とからなり、情報提供者は、契約者に情報を提供し、契約者は、提供される情報を利用して、情報提供者に利用料金を支払うような情報提供システムであって、

前記 1 以上の情報提供者側にはそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する配信手段が設けられ、

前記契約者側には、情報サーバおよびオフライン端末が設けられ、

前記情報サーバは、

前記 1 以上の情報提供者が提供する情報を受信する受信手段と、

前記受信手段が受信した情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成し、かつ、作成した実行権データおよび当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定する課金手段と、

前記課金手段が算定して得られた利用料金を記録するデータ記録手段とを備え、

前記オフライン端末は、前記情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記情報サーバから伝達された情報の利用を許可することを特徴とする情報提供システム。

【請求項 12】 前記 1 以上の情報提供者が提供する情報は、それぞれ暗号化されており、

前記情報サーバは、前記受信手段が受信した情報を復号する第 1 の復号手段をさらに備えることを特徴とする、請求項 11 に記載の情報提供システム。

【請求項 13】 前記情報サーバは、前記第 1 の復号手段が復号して得られた情報を、所定の方式で再暗号化する共通暗号化手段をさらに備え、

前記オフライン端末は、前記情報サーバから伝達された、再暗号化された情報を、前記情報サーバから伝達された実行権データが所定の条件を満たす場合に復号する第 2 の復号手段を備えることを特徴とする、請求項 12 に記載の情報提供システム。

【請求項 14】 前記情報サーバは、

乱数を発生する乱数発生手段と、

前記第 1 の復号手段が復号して得られた情報を、前記乱数発生手段が発生する乱数で再暗号化する共通暗号化手段とをさらに備え、

前記オフライン端末は、前記情報サーバから伝達された、再暗号化された情報を、前記情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記情報サーバから伝達された乱数で復号する第 2 の復号手段を備えることを特徴とする、請求項 12 に記載の情報提供システム。

【請求項 15】 前記共通暗号化手段が再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、前記乱数発生手段が発生した乱数および前記課金手段が作成した実行権データは、記録内容の解析／変更が困難な携帯型記録媒体を介して、それぞれ前記オフライン端末に伝達されることを特徴とする、請求項 14 に記載の情報提供システム。

【請求項 16】 1 以上の情報提供者と契約者とからなり、情報提供者は、契約者に情報を提供し、契約者は、提供される情報を利用して、情報提供者に利用料金を支払うような情報提供システムの契約者側に設けられる情報サーバであって、

前記 1 以上の情報提供者はそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信し、

前記契約者側には、さらに、伝達された実行権データが所定の条件を満たす場合に、伝達された情報の利用を許可する機能を有するオフライン端末が設けられ、

前記 1 以上の情報提供者が提供する情報を受信する受信手段と、

前記受信手段が受信した情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成し、かつ、作成した実行権データおよび当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定する課金手段と、

前記課金手段が算定して得られた利用料金を記録するデータ記録手段とを備える情報サーバ。

【請求項 17】 前記 1 以上の情報提供者が提供する情報は、それぞれ暗号化されており、

前記受信手段が受信した情報を復号する復号手段をさらに備えることを特徴とする、請求項 16 に記載の情報サーバ。

【請求項 18】 前記オフライン端末は、前記情報サーバから伝達された、再暗号化された情報を、前記情報サーバから伝達された実行権データが所定の条件を満たす場合に復号する機能を有しており、

前記復号手段が復号して得られた情報を、所定の方式で再暗号化する共通暗号化手段をさらに備えることを特徴とする、請求項 17 に記載の情報サーバ。

【請求項 19】 前記オフライン端末は、前記情報サーバから伝達された、再暗号化された情報を、前記情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記情報サーバから伝達された乱数で復号する機能を有しており、

乱数を発生する乱数発生手段と、

前記復号手段が復号して得られた情報を、前記乱数発生手段が発生する乱数で再暗号化する共通暗号化手段とをさらに備えることを特徴とする、請求項 17 に記載の情報サーバ。

【請求項 20】 前記共通暗号化手段が再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、前記乱数発生手段が発生した乱数および前記課金手段が作成した実行権データは、記録内容の解析／変更が困難な携帯型記録媒体を介して、それぞれ前記オフライン端末に伝達されることを特徴とする、請求項 19 に記載の情報サーバ。

【請求項 21】 1 以上の情報提供者と契約者とは、情報提供者は、契約者に情報を提供し、契約者は、提供される情報を利用して、情報提供者に利用料金を支払うような情報提供システムの契約者側に設けられるオフライン端末であって、

前記 1 以上の情報提供者はそれぞれ、提供すべき情報

に、当該情報の利用料金を算定するための課金基準データを付加して配信し、

前記契約者側には、さらに、前記 1 以上の情報提供者が提供する情報を受信し、かつ受信した情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成し、かつ作成した実行権データおよび当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定し、かつ算定して得た利用料金を記録する機能を有する情報サーバが設けられ、

10 前記情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記情報サーバから伝達された情報の利用を許可することを特徴とするオフライン端末。

【請求項 22】 前記 1 以上の情報提供者が提供する情報は、それぞれ暗号化されており、

前記情報サーバは、受信した情報を復号する機能をさらに有することを特徴とする、請求項 21 に記載のオフライン端末。

【請求項 23】 前記情報サーバは、復号して得た情報を、所定の方式で再暗号化する機能をさらに有し、

20 前記情報サーバから伝達された、再暗号化された情報を、前記情報サーバから伝達された実行権データが所定の条件を満たす場合に復号する復号手段を備えることを特徴とする、請求項 22 に記載のオフライン端末。

【請求項 24】 前記情報サーバは、乱数を発生し、かつ、復号して得た情報を、当該乱数で再暗号化する機能をさらに有し、

前記情報サーバから伝達された、再暗号化された情報を、前記情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記情報サーバから伝達された乱数で復号する復号手段を備えることを特徴とする、請求項 22 に記載のオフライン端末。

【請求項 25】 前記情報サーバが再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、前記情報サーバが発生した乱数および作成した実行権データは、記録内容の解析／変更が困難な携帯型記録媒体を介して、それぞれ前記オフライン端末に伝達されることを特徴とする、請求項 24 に記載のオフライン端末。

【請求項 26】 1 以上の情報提供者と第 1 および第 2 の契約者とは、情報提供者は、第 1 の契約者に情報を提供し、第 1 の契約者は、提供される情報を第 2 の契約者に再提供して、第 1 の契約者が情報提供者に利用料金を支払うような情報提供システムであって、前記 1 以上の情報提供者側にはそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する配信手段が設けられ、前記第 1 の契約者側には情報サーバが、前記第 2 の契約者側には 1 以上の端末がそれぞれ設けられ、

前記情報サーバは、

50 前記 1 以上の情報提供者が提供する情報を受信する受信

手段と、

前記受信手段が受信した情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成し、かつ、作成した実行権データおよび当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定する課金手段と、

前記課金手段が算定して得られた利用料金を記録するデータ記録手段とを備え、

前記1以上の端末はそれぞれ、前記情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記情報サーバから伝達された情報の利用を許可することを特徴とする情報提供システム。

【請求項27】 前記1以上の情報提供者が提供する情報は、それぞれ暗号化されており、

前記情報サーバは、前記受信手段が受信した情報を復号する第1の復号手段をさらに備えることを特徴とする、請求項26に記載の情報提供システム。

【請求項28】 前記情報サーバは、前記第1の復号手段が復号して得られた情報を、所定の方式で再暗号化する共通暗号化手段をさらに備え、

前記1以上の端末はそれぞれ、前記情報サーバから伝達された、再暗号化された情報を、前記情報サーバから伝達された実行権データが所定の条件を満たす場合に復号する第2の復号手段を備えることを特徴とする、請求項27に記載の情報提供システム。

【請求項29】 前記情報サーバは、

乱数を発生する乱数発生手段と、

前記第1の復号手段が復号して得られた情報を、前記乱数発生手段が発生する乱数で再暗号化する共通暗号化手段とをさらに備え、

前記1以上の端末はそれぞれ、前記情報サーバから伝達された、再暗号化された情報を、前記情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記情報サーバから伝達された乱数で復号する第2の復号手段を備えることを特徴とする、請求項27に記載の情報提供システム。

【請求項30】 前記共通暗号化手段が再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、前記乱数発生手段が発生した乱数および前記課金手段が作成した実行権データは、記録内容の解析／変更が困難な携帯型記録媒体を介して、それぞれ前記第2の契約者側に伝達されることを特徴とする、請求項29に記載の情報提供システム。

【請求項31】 前記情報サーバは、

乱数を発生する乱数発生手段と、

前記第1の復号手段が復号して得られた情報を、前記乱数発生手段が発生する乱数で再暗号化し、かつ、前記乱数発生手段が発生した乱数および前記課金手段が作成した実行権データを所定の方式で暗号化する共通暗号化手段とをさらに備え、

前記1以上の端末はそれぞれ、前記情報サーバから伝達された、暗号化された乱数および実行権データを復号し、かつ、前記情報サーバから伝達された、再暗号化された情報を、復号して得た実行権データが所定の条件を満たす場合に、復号して得た乱数で復号する第2の復号手段を備えることを特徴とする、請求項27に記載の情報提供システム。

【請求項32】 前記共通暗号化手段が再暗号化して得られた情報ならびに前記共通暗号化手段が暗号化して得られた乱数および実行権データは、伝送速度が比較的大きい伝送路を介して、前記第2の契約者側に伝達されることを特徴とする、請求項31に記載の情報提供システム。

【請求項33】 前記共通暗号化手段が再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、前記共通暗号化手段が暗号化して得られた乱数および実行権データは、伝送速度が比較的小さい伝送路を介して、それぞれ前記第2の契約者側に伝達されることを特徴とする、請求項31に記載の情報提供システム。

【請求項34】 1以上の情報提供者と第1および第2の契約者とからなり、情報提供者は、第1の契約者に情報を提供し、第1の契約者は、提供される情報を第2の契約者に再提供して、第1の契約者が情報提供者に利用料金を支払うような情報提供システムの第1の契約者側に設けられる情報サーバであって、前記1以上の情報提供者はそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信し、

前記第2の契約者側には、前記情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記情報サーバから伝達された情報の利用を許可する機能を有する1以上の端末が設けられており、

前記1以上の情報提供者が提供する情報を受信する受信手段と、

前記受信手段が受信した情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成し、かつ、作成した実行権データおよび当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定する課金手段と、

前記課金手段が算定して得られた利用料金を記録するデータ記録手段とを備える情報サーバ。

【請求項35】 前記1以上の情報提供者が提供する情報は、それぞれ暗号化されており、

前記受信手段が受信した情報を復号する復号手段をさらに備えることを特徴とする、請求項34に記載の情報サーバ。

【請求項36】 前記1以上の端末はそれぞれ、前記情報サーバから伝達された、再暗号化された情報を、前記情報サーバから伝達された実行権データが所定の条件を

満たす場合に復号する機能を有しており、前記復号手段が復号して得られた情報を、所定の方式で再暗号化する共通暗号化手段をさらに備えることを特徴とする、請求項 3 5 に記載の情報サーバ。

【請求項 3 7】 前記 1 以上の端末はそれぞれ、前記情報サーバから伝達された、再暗号化された情報を、前記情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記情報サーバから伝達された乱数で復号する機能を有しており、

乱数を発生する乱数発生手段と、前記復号手段が復号して得られた情報を、前記乱数発生手段が発生する乱数で再暗号化する共通暗号化手段とをさらに備えることを特徴とする、請求項 3 5 に記載の情報サーバ。

【請求項 3 8】 前記共通暗号化手段が再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、前記乱数発生手段が発生した乱数および前記課金手段が作成した実行権データは、記録内容の解析／変更が困難な携帯型記録媒体を介して、それぞれ前記第 2 の契約者側に伝達されることを特徴とする、請求項 3 7 に記載の情報サーバ。

【請求項 3 9】 前記 1 以上の端末はそれぞれ、前記情報サーバから伝達された、暗号化された乱数および実行権データを復号し、かつ、前記情報サーバから伝達された、再暗号化された情報を、復号して得た実行権データが所定の条件を満たす場合に、復号して得た乱数で復号する機能を有しており、

乱数を発生する乱数発生手段と、前記復号手段が復号して得られた情報を、前記乱数発生手段が発生する乱数で再暗号化し、かつ、前記乱数発生手段が発生した乱数および前記課金手段が作成した実行権データを所定の方式で暗号化する共通暗号化手段とをさらに備えることを特徴とする、請求項 3 5 に記載の情報サーバ。

【請求項 4 0】 前記共通暗号化手段が再暗号化して得られた情報ならびに前記共通暗号化手段が暗号化して得られた乱数および実行権データは、伝送速度が比較的大きい伝送路を介して、前記第 2 の契約者側に伝達されることを特徴とする、請求項 3 9 に記載の情報サーバ。

【請求項 4 1】 前記共通暗号化手段が再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、前記共通暗号化手段が暗号化して得られた乱数および実行権データは、伝送速度が比較的小さい伝送路を介して、それぞれ前記第 2 の契約者側に伝達されることを特徴とする、請求項 3 9 に記載の情報サーバ。

【請求項 4 2】 1 以上の情報提供者と第 1 および第 2 の契約者とからなり、情報提供者は、第 1 の契約者に情報を提供し、第 1 の契約者は、提供される情報を第 2 の契約者に再提供して、第 1 の契約者が情報提供者に利用料金を支払うような情報提供システムの第 2 の契約者側

に設けられる端末であって、

前記 1 以上の情報提供者はそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信し、

前記第 1 の契約者側には、前記 1 以上の情報提供者が提供する情報を受信し、かつ受信した情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成し、かつ作成した実行権データおよび当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定し、かつ算定して得た利用料金を記録する機能を有する情報サーバが設けられ、

前記情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記情報サーバから伝達された情報の利用を許可することを特徴とする端末。

【請求項 4 3】 前記 1 以上の情報提供者が提供する情報は、それぞれ暗号化されており、

前記情報サーバは、受信した情報を復号する機能をさらに有することを特徴とする、請求項 4 2 に記載の端末。

【請求項 4 4】 前記情報サーバは、復号して得た情報を所定の方式で再暗号化する機能をさらに有し、前記情報サーバから伝達された、再暗号化された情報を、前記情報サーバから伝達された実行権データが所定の条件を満たす場合に復号する復号手段を備えることを特徴とする、請求項 4 3 に記載の端末。

【請求項 4 5】 前記情報サーバは、乱数を発生し、かつ復号して得た情報を当該乱数で再暗号化する機能をさらに有し、

前記情報サーバから伝達された、再暗号化された情報を、前記情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記情報サーバから伝達された乱数で復号する復号手段を備えることを特徴とする、請求項 4 3 に記載の端末。

【請求項 4 6】 前記情報サーバが再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、前記情報サーバが発生した乱数および作成した実行権データは、記録内容の解析／変更が困難な携帯型記録媒体を介して、それぞれ前記第 2 の契約者側に伝達されることを特徴とする、請求項 4 5 に記載の端末。

【請求項 4 7】 前記情報サーバは、乱数を発生し、かつ復号して得た情報を当該乱数で再暗号化し、かつ当該乱数および作成した実行権データを所定の方式で暗号化する機能をさらに有し、

前記情報サーバから伝達された、暗号化された乱数および実行権データを復号し、かつ、前記情報サーバから伝達された、再暗号化された情報を、復号して得た実行権データが所定の条件を満たす場合に、復号して得た乱数で復号する復号手段を備えることを特徴とする、請求項 4 3 に記載の端末。

【請求項 4 8】 前記情報サーバが再暗号化して得られた情報ならびに前記情報サーバが暗号化して得られた乱

数および実行権データは、伝送速度が比較的大きい伝送路を介して、前記第2の契約者側に伝達されることを特徴とする、請求項47に記載の端末。

【請求項49】 前記情報サーバが再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、前記情報サーバが暗号化して得られた乱数および実行権データは、伝送速度が比較的小さい伝送路を介して、それぞれ前記第2の契約者側に伝達されることを特徴とする、請求項47に記載の端末。

【請求項50】 1以上の情報提供者と第1および第2の契約者とは、情報提供者は、第1の契約者に情報を提供し、第1の契約者は、提供される情報を第2の契約者に再提供して、第2の契約者が情報提供者に利用料金を支払うような情報提供システムであって、前記1以上の情報提供者側にはそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する配信手段が設けられ、前記第1の契約者側には第1の情報サーバが、前記第2の契約者側には第2の情報サーバおよび当該情報サーバに情報伝達可能に接続された1以上の端末がそれぞれ設けられ、前記第1の情報サーバは、前記1以上の情報提供者が提供する情報を受信する受信手段と、前記受信手段が受信した情報を利用可能な端末を制限するための実行権データを作成する実行権データ作成手段とを備え、前記第2の情報サーバは、前記第1の情報サーバから伝達された情報に付加された課金基準データに基づいて、当該情報の利用料金を算定する課金手段と、前記課金手段が算定して得られた利用料金を記録するデータ記録手段とを備え、前記1以上の端末はそれぞれ、前記第1の情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記第1の情報サーバから伝達された情報の利用を許可することを特徴とする情報提供システム。

【請求項51】 前記1以上の情報提供者が提供する情報は、それぞれ暗号化されており、前記第1の情報サーバは、前記受信手段が受信した情報を復号する第1の復号手段をさらに備えることを特徴とする、請求項50に記載の情報提供システム。

【請求項52】 前記第1の情報サーバは、前記第1の復号手段が復号して得られた情報を、所定の方式で再暗号化する共通暗号化手段をさらに備え、前記1以上の端末はそれぞれ、前記第1の情報サーバから伝達された、再暗号化された情報を、前記第1の情報サーバから伝達された実行権データが所定の条件を満たす場合に復号する第2の復号手段を備えることを特徴とする、請求項51に記載の情報提供システム。

【請求項53】 前記第1の情報サーバは、

乱数を発生する乱数発生手段と、

前記第1の復号手段が復号して得られた情報を、前記乱数発生手段が発生する乱数で再暗号化する共通暗号化手段とをさらに備え、

前記1以上の端末はそれぞれ、前記第1の情報サーバから伝達された、再暗号化された情報を、前記第1の情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記第1の情報サーバから伝達された乱数で復号する第2の復号手段を備えることを特徴とする、請求項51に記載の情報提供システム。

【請求項54】 前記共通暗号化手段が再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、前記乱数発生手段が発生した乱数および前記課金手段が作成した実行権データは、記録内容の解析／変更が困難な携帯型記録媒体を介して、それぞれ前記第2の契約者側に伝達されることを特徴とする、請求項53に記載の情報提供システム。

【請求項55】 前記第1の情報サーバは、

乱数を発生する乱数発生手段と、

前記第1の復号手段が復号して得られた情報を、前記乱数発生手段が発生する乱数で再暗号化し、かつ、前記乱数発生手段が発生した乱数および前記実行権データ作成手段が作成した実行権データを所定の方式で暗号化する共通暗号化手段とをさらに備え、

前記1以上の端末はそれぞれ、前記第1の情報サーバから伝達された、暗号化された乱数および実行権データを復号し、かつ、前記第1の情報サーバから伝達された、再暗号化された情報を、復号して得た実行権データが所定の条件を満たす場合に、復号して得た乱数で復号する第2の復号手段を備えることを特徴とする、請求項51に記載の情報提供システム。

【請求項56】 前記共通暗号化手段が再暗号化して得られた情報ならびに前記共通暗号化手段が暗号化して得られた乱数および実行権データは、伝送速度が比較的大きい伝送路を介して、前記第2の契約者側に伝達されることを特徴とする、請求項55に記載の情報提供システム。

【請求項57】 前記共通暗号化手段が再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、前記共通暗号化手段が暗号化して得られた乱数および実行権データは、伝送速度が比較的小さい伝送路を介して、それぞれ前記第2の契約者側に伝達されることを特徴とする、請求項55に記載の情報提供システム。

【請求項58】 1以上の情報提供者と第1および第2の契約者とは、情報提供者は、第1の契約者に情報を提供し、第1の契約者は、提供される情報を第2の契約者に再提供して、第2の契約者が情報提供者に利用料金を支払うような情報提供システムの第1の契約者側

に設けられる情報サーバであって、
 前記1以上の情報提供者はそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信し、
 前記第2の契約者側には、伝達された情報に付加された課金基準データに基づいて、当該情報の利用料金を算定し、かつ算定して得た利用料金を記録する機能を有する他の情報サーバ、および当該他の情報サーバに情報伝達可能に接続され、前記情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記情報サーバから伝達された情報の利用を許可する機能を有する1以上の端末が設けられており、
 前記1以上の情報提供者が提供する情報を受信する受信手段と、
 前記受信手段が受信した情報を利用可能な端末を制限するための実行権データを作成する実行権データ作成手段とを備える情報サーバ。

【請求項59】 前記1以上の情報提供者が提供する情報は、それぞれ暗号化されており、
 前記受信手段が受信した情報を復号する復号手段をさらに備えることを特徴とする、請求項58に記載の情報サーバ。

【請求項60】 前記1以上の端末はそれぞれ、前記情報サーバから伝達された、再暗号化された情報を、前記情報サーバから伝達された実行権データが所定の条件を満たす場合に復号する機能を有しており、
 前記復号手段が復号して得られた情報を、所定の方式で再暗号化する共通暗号化手段をさらに備えることを特徴とする、請求項59に記載の情報サーバ。

【請求項61】 前記1以上の端末はそれぞれ、前記情報サーバから伝達された、再暗号化された情報を、前記情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記情報サーバから伝達された乱数で復号する機能を有しており、
 乱数を発生する乱数発生手段と、
 前記復号手段が復号して得られた情報を、前記乱数発生手段が発生する乱数で再暗号化する共通暗号化手段とをさらに備えることを特徴とする、請求項59に記載の情報サーバ。

【請求項62】 前記共通暗号化手段が再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、前記乱数発生手段が発生した乱数および前記実行権データ作成手段が作成した実行権データは、記録内容の解析／変更が困難な携帯型記録媒体を介して、それぞれ前記第2の契約者側に伝達されることを特徴とする、請求項61に記載の情報サーバ。

【請求項63】 前記1以上の端末はそれぞれ、前記情報サーバから伝達された、暗号化された乱数および実行権データを復号し、かつ、前記情報サーバから伝達された、再暗号化された情報を、復号して得た実行権データ

が所定の条件を満たす場合に、復号して得た乱数で復号する機能を有しており、
 乱数を発生する乱数発生手段と、
 前記復号手段が復号して得られた情報を、前記乱数発生手段が発生する乱数で再暗号化し、かつ、前記乱数発生手段が発生した乱数および前記実行権データ作成手段が作成した実行権データを所定の方式で暗号化する共通暗号化手段とをさらに備えることを特徴とする、請求項59に記載の情報サーバ。

10 【請求項64】 前記共通暗号化手段が再暗号化して得られた情報ならびに前記共通暗号化手段が暗号化して得られた乱数および実行権データは、伝送速度が比較的大きい伝送路を介して、前記第2の契約者側に伝達されることを特徴とする、請求項63に記載の情報サーバ。

【請求項65】 前記共通暗号化手段が再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、前記共通暗号化手段が暗号化して得られた乱数および実行権データは、伝送速度が比較的小さい伝送路を介して、それぞれ前記第2の契約者側に伝達されることを特徴とする、請求項63に記載の情報サーバ。

20 【請求項66】 1以上の情報提供者と第1および第2の契約者とからなり、情報提供者は、第1の契約者に情報を提供し、第1の契約者は、提供される情報を第2の契約者に再提供して、第2の契約者が情報提供者に利用料金を支払うような情報提供システムの第2の契約者側に設けられる情報サーバであって、
 前記1以上の情報提供者はそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信し、

30 前記第1の契約者側には、前記1以上の情報提供者が提供する情報を受信し、かつ受信した情報を利用可能な端末を制限するための実行権データを作成する機能を有する他の情報サーバが設けられており、
 前記第2の契約者側には、さらに、前記他の情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記他の情報サーバから伝達された情報の利用を許可する機能を有する1以上の端末が設けられており、
 前記他の情報サーバから伝達された情報に付加された課金基準データに基づいて、当該情報の利用料金を算定する課金手段と、
 前記課金手段が算定して得られた利用料金を記録するデータ記録手段とを備える情報サーバ。

40 【請求項67】 前記1以上の情報提供者が提供する情報は、それぞれ暗号化されており、
 前記他の情報サーバは、受信した情報を復号する機能をさらに有することを特徴とする、請求項66に記載の情報サーバ。

【請求項68】 前記他の情報サーバは、復号して得た情報を所定の方式で再暗号化する機能をさらに有し、
 前記1以上の端末はそれぞれ、前記他の情報サーバから

50

伝達された、再暗号化された情報を、前記他の情報サーバから伝達された実行権データが所定の条件を満たす場合に復号する機能を有することを特徴とする、請求項67に記載の情報サーバ。

【請求項69】 前記他の情報サーバは、乱数を発生し、かつ復号して得た情報を当該乱数で再暗号化する機能をさらに有し、

前記1以上の端末はそれぞれ、前記他の情報サーバから伝達された、再暗号化された情報を、前記他の情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記他の情報サーバから伝達された乱数で復号する機能を有することを特徴とする、請求項67に記載の情報サーバ。

【請求項70】 前記他の情報サーバが再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、前記他の情報サーバが発生した乱数および作成した実行権データは、記録内容の解析／変更が困難な携帯型記録媒体を介して、それぞれ前記第2の契約者側に伝達されることを特徴とする、請求項69に記載の情報サーバ。

【請求項71】 前記他の情報サーバは、乱数を発生し、かつ復号して得た情報を当該乱数で再暗号化し、かつ当該乱数および作成した実行権データを所定の方式で暗号化する機能をさらに有し、

前記1以上の端末はそれぞれ、前記他の情報サーバから伝達された、暗号化された乱数および実行権データを復号し、かつ、前記他の情報サーバから伝達された、再暗号化された情報を、復号して得た実行権データが所定の条件を満たす場合に、復号して得た乱数で復号する機能を有することを特徴とする、請求項67に記載の情報サーバ。

【請求項72】 前記他の情報サーバが再暗号化して得られた情報ならびに前記他の情報サーバが暗号化して得られた乱数および実行権データは、伝送速度が比較的大きい伝送路を介して、前記第2の契約者側に伝達されることを特徴とする、請求項71に記載の情報サーバ。

【請求項73】 前記他の情報サーバが再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、前記他の情報サーバが暗号化して得られた乱数および実行権データは、伝送速度が比較的小さい伝送路を介して、それぞれ前記第2の契約者側に伝達されることを特徴とする、請求項71に記載の情報サーバ。

【請求項74】 1以上の情報提供者と第1および第2の契約者とからなり、情報提供者は、第1の契約者に情報を提供し、第1の契約者は、提供される情報を第2の契約者に再提供して、第2の契約者が情報提供者に利用料金を支払うような情報提供システムの第2の契約者側に設けられる端末であって、
前記1以上の情報提供者はそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準デ

タを付加して配信し、

前記第1の契約者側には、前記1以上の情報提供者が提供する情報を受信し、かつ受信した情報を利用可能な端末を制限するための実行権データを作成する機能を有する第1の情報サーバが設けられており、

前記第2の契約者側には、さらに、前記第1の情報サーバから伝達された情報に付加された課金基準データに基づいて、当該情報の利用料金を算定し、かつ算定して得た利用料金を記録する機能を有する第2の情報サーバが設けられており、

前記第1の情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記第1の情報サーバから伝達された情報の利用を許可することを特徴とする端末。

【請求項75】 前記1以上の情報提供者が提供する情報は、それぞれ暗号化されており、

前記第1の情報サーバは、受信した情報を復号する機能をさらに有することを特徴とする、請求項74に記載の端末。

【請求項76】 前記第1の情報サーバは、復号して得た情報を所定の方式で再暗号化する機能をさらに有し、前記第1の情報サーバから伝達された、再暗号化された情報を、前記第1の情報サーバから伝達された実行権データが所定の条件を満たす場合に復号する復号手段を備えることを特徴とする、請求項75に記載の端末。

【請求項77】 前記第1の情報サーバは、乱数を発生し、かつ復号して得た情報を当該乱数で再暗号化する機能をさらに有し、

前記第1の情報サーバから伝達された、再暗号化された情報を、前記第1の情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記第1の情報サーバから伝達された乱数で復号する復号手段を備えることを特徴とする、請求項75に記載の端末。

【請求項78】 前記第1の情報サーバが再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、前記第1の情報サーバが発生した乱数および作成した実行権データは、記録内容の解析／変更が困難な携帯型記録媒体を介して、それぞれ前記第2の契約者側に伝達されることを特徴とする、請求項77に記載の端末。

【請求項79】 前記第1の情報サーバは、乱数を発生し、かつ復号して得た情報を当該乱数で再暗号化し、かつ当該乱数および作成した実行権データを所定の方式で暗号化する機能をさらに有し、

前記第1の情報サーバから伝達された、暗号化された乱数および実行権データを復号し、かつ前記第1の情報サーバから伝達された、再暗号化された情報を、復号して得た実行権データが所定の条件を満たす場合に、復号して得た乱数で復号する復号手段を備えることを特徴とする、請求項75に記載の端末。

【請求項80】 前記第1の情報サーバが再暗号化して

得られた情報ならびに前記第1の情報サーバが暗号化して得られた乱数および実行権データは、伝送速度が比較的大きい伝送路を介して、前記第2の契約者側に伝達されることを特徴とする、請求項79に記載の端末。

【請求項81】 前記第1の情報サーバが再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、前記第1の情報サーバが暗号化して得られた乱数および実行権データは、伝送速度が比較的小さい伝送路を介して、それぞれ前記第2の契約者側に伝達されることを特徴とする、請求項79に記載の端末。

【請求項82】 1以上の情報提供者と契約者とは、情報提供者は、契約者に情報を提供し、契約者は、提供される情報を利用して、情報提供者に利用料金を支払うような情報提供方法であって、前記1以上の情報提供者はそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信し、前記契約者側には、情報サーバおよび当該情報サーバに情報伝達可能に接続された1以上の端末が設けられ、前記情報サーバは、前記1以上の情報提供者が提供する情報を受信し、受信した情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定し、算定して得た利用料金を記録することを特徴とする情報提供方法。

【請求項83】 前記1以上の情報提供者が提供する情報は、それぞれ暗号化されており、前記情報サーバは、さらに、受信した情報を復号することを特徴とする、請求項82に記載の情報提供方法。

【請求項84】 前記情報サーバは、前記1以上の端末毎の秘密鍵を記憶しており、さらに、復号して得た情報を、当該秘密鍵でそれぞれ再暗号化し、前記1以上の端末はそれぞれ、自己の秘密鍵を記憶しており、前記情報サーバから伝達された、再暗号化された情報を、当該秘密鍵で復号することを特徴とする、請求項83に記載の情報提供方法。

【請求項85】 前記情報サーバは、前記1以上の端末毎の秘密鍵を記憶しており、さらに、乱数を発生し、復号して得た情報を、当該乱数で再暗号化し、当該乱数を、当該秘密鍵でそれぞれ暗号化し、前記1以上の端末はそれぞれ、自己の秘密鍵を記憶しており、前記情報サーバから伝達された、暗号化された乱数を、当該秘密鍵で復号し、前記情報サーバから伝達された、再暗号化された情報を、復号して得た乱数で復号することを特徴とする、請求項83に記載の情報提供方法。

【請求項86】 前記1以上の情報提供者はそれぞれ、提供すべき情報に、記録を許可するか否かを示す記録許

可フラグをさらに付加して配信し、前記情報サーバは、受信した情報に付加されている記録許可フラグが、記録を許可するものである場合に、当該情報を記録し、記録した情報が、前記1以上の端末に伝達される毎に、当該情報の利用料金を算定することを特徴とする、請求項82に記載の情報提供方法。

【請求項87】 前記1以上の情報提供者が提供する情報は、それぞれ暗号化されており、

10 前記情報サーバは、さらに、記録した情報を復号することを特徴とする、請求項86に記載の情報提供方法。

【請求項88】 前記情報サーバは、前記1以上の端末毎の秘密鍵を記憶しており、さらに、復号して得た情報を、当該秘密鍵でそれぞれ再暗号化し、前記1以上の端末はそれぞれ、自己の秘密鍵を記憶しており、前記情報サーバから伝達された、再暗号化された情報を、当該秘密鍵で復号することを特徴とする、請求項87に記載の情報提供方法。

【請求項89】 前記情報サーバは、前記1以上の端末毎の秘密鍵を記憶しており、さらに、乱数を発生し、復号して得た情報を、当該乱数で再暗号化し、当該乱数を、当該秘密鍵でそれぞれ暗号化し、前記1以上の端末はそれぞれ、自己の秘密鍵を記憶しており、前記情報サーバから伝達された、暗号化された乱数を、当該秘密鍵で復号し、前記情報サーバから伝達された、再暗号化された情報を、復号して得た乱数で復号することを特徴とする、請求項87に記載の情報提供方法。

【請求項90】 1以上の情報提供者と契約者とは、情報提供者は、契約者に情報を提供し、契約者は、提供される情報を利用して、情報提供者に利用料金を支払うような情報提供方法であって、前記1以上の情報提供者はそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信し、前記契約者側には、情報サーバおよびオフライン端末が設けられ、

40 前記情報サーバは、前記1以上の情報提供者が提供する情報を受信し、受信した情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成し、作成した実行権データおよび受信した情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定し、算定して得た利用料金を記録し、前記オフライン端末は、前記情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記情報サーバから伝達された情報の利用を許可することを特徴と

する情報提供方法。

【請求項 9 1】 前記 1 以上の情報提供者が提供する情報は、それぞれ暗号化されており、前記情報サーバは、さらに、受信した情報を復号することを特徴とする、請求項 9 0 に記載の情報提供方法。

【請求項 9 2】 前記情報サーバは、さらに、復号して得た情報を所定の方式で再暗号化し、前記オフライン端末は、前記情報サーバから伝達された、再暗号化された情報を、前記情報サーバから伝達された実行権データが所定の条件を満たす場合に復号することを特徴とする、請求項 9 1 に記載の情報提供方法。

【請求項 9 3】 前記情報サーバは、さらに、乱数を発生し、復号して得た情報を、当該乱数で再暗号化し、前記オフライン端末は、前記情報サーバから伝達された、再暗号化された情報を、前記情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記情報サーバから伝達された乱数で復号することを特徴とする、請求項 9 1 に記載の情報提供方法。

【請求項 9 4】 前記情報サーバが再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、前記情報サーバが発生した乱数および作成した実行権データは、記録内容の解析／変更が困難な携帯型記録媒体を介して、それぞれ前記オフライン端末に伝達されることを特徴とする、請求項 9 3 に記載の情報提供方法。

【請求項 9 5】 1 以上の情報提供者と第 1 および第 2 の契約者とからなり、情報提供者は、第 1 の契約者に情報を提供し、第 1 の契約者は、提供される情報を第 2 の契約者に再提供して、第 1 または第 2 の契約者のいずれかが、情報提供者に利用料金を支払うような情報提供方法であって、前記 1 以上の情報提供者はそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信し、前記第 1 の契約者側には第 1 の情報サーバが、前記第 2 の契約者側には、第 2 の情報サーバおよび当該サーバに情報伝達可能に接続された 1 以上の端末が、それぞれ設けられ、前記第 1 の契約者に課金する場合、前記第 1 の情報サーバは、前記 1 以上の情報提供者が提供する情報を受信し、受信した情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成し、作成した実行権データおよび受信した情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定し、算定して得た利用料金を記録し、前記 1 以上の端末はそれぞれ、前記第 1 の情報サーバから伝達された実行権データが所定の条件を満たす場合

に、前記第 1 の情報サーバから伝達された情報の利用を許可し、

前記第 2 の契約者に課金する場合には、

前記第 1 の情報サーバは、

前記 1 以上の情報提供者が提供する情報を受信し、受信した情報を利用可能な端末を制限するための実行権データを作成し、

前記第 2 の情報サーバは、

前記第 1 の情報サーバから伝達された情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定し、

算定して得た利用料金を記録し、

前記 1 以上の端末はそれぞれ、

前記第 1 の情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記第 1 の情報サーバから伝達された情報の利用を許可することを特徴とする情報提供方法。

【請求項 9 6】 前記 1 以上の情報提供者が提供する情報は、それぞれ暗号化されており、

前記第 1 の情報サーバは、さらに、受信した情報を復号することを特徴とする、請求項 9 5 に記載の情報提供方法。

【請求項 9 7】 前記第 1 の情報サーバは、さらに、復号して得た情報を所定の方式で再暗号化し、前記 1 以上の端末はそれぞれ、前記第 1 の情報サーバから伝達された、再暗号化された情報を、前記第 1 の情報サーバから伝達された実行権データが所定の条件を満たす場合に復号することを特徴とする、請求項 9 6 に記載の情報提供方法。

【請求項 9 8】 前記第 1 の情報サーバは、さらに、乱数を発生し、復号して得た情報を、当該乱数で再暗号化し、前記 1 以上の端末はそれぞれ、前記第 1 の情報サーバから伝達された、再暗号化された情報を、前記第 1 の情報サーバから伝達された実行権データが所定の条件を満たす場合に、前記第 1 の情報サーバから伝達された乱数で復号することを特徴とする、請求項 9 6 に記載の情報提供方法。

【請求項 9 9】 前記第 1 の情報サーバが再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、前記第 1 の情報サーバが発生した乱数および作成した実行権データは、記録内容の解析／変更が困難な携帯型記録媒体を介して、それぞれ前記第 2 の契約者側に伝達されることを特徴とする、請求項 9 8 に記載の情報提供方法。

【請求項 100】 前記第 1 の情報サーバは、さらに、乱数を発生し、復号して得た情報を、当該乱数で再暗号化し、当該乱数および作成した実行権データを、所定の方式で暗号化し、

前記１以上の端末はそれぞれ、
前記第１の情報サーバから伝達された、暗号化された乱数および実行権データを復号し、
前記第１の情報サーバから伝達された、再暗号化された情報を、復号して得た実行権データが所定の条件を満たす場合に、復号して得た乱数で復号することを特徴とする、請求項９６に記載の情報提供方法。

【請求項１０１】 前記第１の情報サーバが再暗号化して得られた情報ならびに前記第１の情報サーバが暗号化して得られた乱数および実行権データは、伝送速度が比較的大きい伝送路を介して、前記第２の契約者側に伝達されることを特徴とする、請求項１００に記載の情報提供方法。

【請求項１０２】 前記第１の情報サーバが再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、前記第１の情報サーバが暗号化して得られた乱数および実行権データは、伝送速度が比較的小さい伝送路を介して、それぞれ前記第２の契約者側に伝達されることを特徴とする、請求項１００に記載の情報提供方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報提供システムに関し、より特定的には、情報提供者が契約者に情報を提供して、利用度合に応じて課金する情報提供システムに関する。

【０００２】

【従来の技術】近年、ＢＳ放送、ＣＳ放送、ディジタルＣＡＴＶなど、有料情報提供サービスが広く行なわれるようになった。こうしたサービスでは、通常、ユーザは、情報提供者に、毎月、一定の金額の利用料金を支払うことにより、情報提供者が提供する情報を、自由に利用することができる。このため、提供される情報を、ＶＴＲ等により記録して繰り返し利用したり、さらには、記録した情報を、他のユーザに貸与あるいは譲渡するような行為が少なからず行われ、情報提供者の利益が守られないという不都合が生じている。

【０００３】そこで、上記のような行為を制限することができる情報提供システムの開発が行われている。以下には、こうしたシステムの一例として、特開平７－１６２８３２号公報に記載されている映像情報伝送装置について説明する。この装置は、映像情報をスクランブルされたままで記録することができ、従って、記録された情報の再生に一定の制限を加えることができる。

【０００４】図６は、上記従来の映像情報伝送装置の構成を示すブロック図である。図６の装置は、送信装置９０１、受信装置９０６および伝送路９０５で構成されている。送信装置９０１は、スクランブル装置９０２、再生限定情報生成装置９０３、多重装置９０４を備えている。受信装置９０６は、分離装置９０７、変換装置９０

８、ＩＣカードＩ／Ｆ９０９、ＩＣカード９１０、ＶＴＲ９１１およびデスクランブル装置９１２を備えている。

【０００５】図６のスクランブル装置９０２は、映像情報をスクランブルする。再生限定情報生成装置９０３は、受信装置９０６での再生を限定するための再生限定情報を生成する。多重化装置９０４は、映像情報と再生限定情報とを多重化する。分離装置９０７は、多重化された情報を、映像情報と再生限定情報とに分離する。変換装置９０８は、映像情報のフォーマットを変換する。ＶＴＲ９１１は、映像情報を記録する。ＩＣカードＩ／Ｆ９０９は、ＩＣカード９１０に再生限定情報を記録する。ＩＣカード９１０は、再生限定情報を格納する。デスクランブル装置９１２は、再生限定情報に基づいて、スクランブルされた映像信号をデスクランブルする。

【０００６】以下には、図６の映像情報伝送装置の動作について説明する。送信装置９０１において、スクランブル装置９０２が映像情報をスクランブルする一方、再生限定情報生成装置９０３は、制御情報に従って、再生限定情報を生成して暗号化するとともに、スクランブル装置９０２に対してスクランブル情報を与える。多重装置９０４は、スクランブル装置９０２が出力する映像情報と、再生限定情報生成装置９０３が与える再生限定情報とを多重化して、伝送路９０５を介して受信装置９０６へ送信する。

【０００７】送信された情報は、受信装置９０６の分離装置９０７により、映像情報と再生限定情報とに分離される。分離して得られた映像情報は、変換装置９０８において、伝送用のフォーマットから記録用のフォーマットに変換された後、ＶＴＲ９１１により、磁気テープに記録される。一方、分離して得られた再生限定情報は、ＩＣカードＩ／Ｆ９０９においてＩＣカード９１０に記録される。ユーザがＩＣカード９１０をデスクランブル装置９１２に接続すると、デスクランブル装置９１２は、ＩＣカード９１０から読み出した再生限定情報が許可する範囲内で、ＶＴＲ９１１に記録された映像情報をデスクランブルする。

【０００８】

【発明が解決しようとする課題】上記のように、図６の装置は、映像情報が録画されて、無制限に再生されるのを防ぐことができる。しかし、情報提供者にとって、ユーザとの間で、毎月の利用料金を予め一定の金額に決めておき、一方で、上記装置等を用いて、情報の利用を、予め定めた利用度合の上限以下に制限するような方法は、必ずしも有益なものとはいえない。ユーザが情報を記録して繰り返し利用したいと希望するのであれば、記録して好きな回数だけ利用してもらい、利用度合に応じて、利用料金を徴収する方がより望ましい。同様に、ユーザが記録した情報を他のユーザに貸与あるいは譲渡したいと望む場合にも、一定の条件の下で、貸与あるいは

譲渡してもらい、利用度合に応じて、いずれかのユーザから利用料金を徴収するのが望ましい。

【0009】また、ユーザにとっても、情報を記録して利用できなかったり、他のユーザが記録した情報を利用できないのは不便であり、また、利用料金を予め一定の金額に決めておくと、情報を利用する頻度によっては、利益にならない場合がある。

【0010】従って、本発明の目的は、情報提供者からユーザに情報を提供して、利用度合に応じて課金することができるような情報提供システムを提供することである。

【0011】また、情報が正規のユーザ以外の者によって利用されたり、課金に関するデータが不正に操作されるようなことがあると、利用度合に応じた課金を正しく行うことができない。

【0012】従って、本発明の他の目的は、上記システムにおいて、情報や課金に関するデータを、より安全に伝達できるようにすることである。

【0013】

【課題を解決するための手段および発明の効果】第1の発明は、1以上の情報提供者と契約者とはなり、情報提供者は、契約者に情報を提供し、契約者は、提供される情報を利用して、情報提供者に利用料金を支払うような情報提供システムであって、1以上の情報提供者側にはそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する配信手段が設けられ、契約者側には、情報サーバおよび当該情報サーバに情報伝達可能に接続された1以上の端末が設けられ、情報サーバは、1以上の情報提供者が提供する情報を受信する受信手段と、受信手段が受信した情報を記録する情報記録手段と、情報記録手段が記録した情報が、1以上の端末に伝達される毎に、当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定する課金手段と、課金手段が算定して得られた利用料金を記録するデータ記録手段とを備えている。

【0014】上記のように、第1の発明では、1以上の情報提供者側に設けられた配信手段は、提供しようとする情報に当該情報の利用料金を算定するための課金基準データを付加して配信する。契約者側には情報サーバおよび1以上の端末が設けられ、情報サーバの受信手段は、1以上の情報提供者が配信する情報を受信する。情報記録手段は、受信手段が受信した情報を記録する。課金手段は、情報記録手段が記録した情報が1以上の端末に伝達される毎に、当該情報に付加された課金基準データに基づいて、当該情報の利用料金を算定する。データ記録手段は、課金手段が算定して得られた利用料金を記録する。なお、記録された利用料金は、所定の方法で情報提供者に通知され、契約者は当該料金を支払うことになる。

【0015】このように、情報サーバは、1以上の情報

提供者が提供する情報を記録する。そして、情報サーバは、記録した情報が1以上の端末に伝達される毎に、当該情報の利用料金を算定し、算定して得た利用料金を記録する。これにより、契約者が情報を記録して繰り返し利用する場合、利用度合に応じた課金ができる。

【0016】第2の発明は、第1の発明において、1以上の情報提供者が提供する情報は、それぞれ暗号化されており、情報サーバは、情報記録手段が記録した情報を復号する第1の復号手段をさらに備えることを特徴としている。

【0017】上記のように、第2の発明では、1以上の情報提供者が提供する情報が暗号化されている場合、情報記録手段は、当該情報を、暗号化されたままで記録する。第1の復号手段は、情報記録手段が記録した情報が、1以上の端末に伝達される際に、当該情報を復号する。

【0018】このように、情報サーバは、提供される情報を暗号化されたままで記録し、当該情報が端末に伝達される際に復号することにより、記録された情報が不正に利用されるのを防ぐことができる。

【0019】第3の発明は、第2の発明において、データ記録手段は、1以上の端末毎の秘密鍵を記憶しており、情報サーバは、第1の復号手段が復号して得られた情報を、データ記録手段が記憶している1以上の端末毎の秘密鍵でそれぞれ再暗号化する共通暗号化手段をさらに備え、1以上の端末はそれぞれ、自己の秘密鍵を記憶しており、情報サーバから伝達された、再暗号化された情報を、当該秘密鍵で復号する第2の復号手段を備えることを特徴としている。

【0020】上記のように、第3の発明では、データ記録手段が1以上の端末毎の秘密鍵を記憶しておき、共通暗号化手段は、第1の復号手段が復号して得られた情報を、当該秘密鍵で再暗号化する。再暗号化された情報が1以上の端末に伝達されると、第2の復号手段は、伝達された、再暗号化された情報を、記憶している自己の秘密鍵で復号する。これにより、情報サーバから1以上の端末に、安全に情報を伝達できる。

【0021】第4の発明は、第2の発明において、データ記録手段は、1以上の端末毎の秘密鍵を記憶しており、情報サーバは、乱数を発生する乱数発生手段と、第1の復号手段が復号して得られた情報を、乱数発生手段が発生する乱数で再暗号化し、かつ、当該乱数を、データ記録手段が記憶している1以上の端末毎の秘密鍵でそれぞれ暗号化する共通暗号化手段とをさらに備え、1以上の端末はそれぞれ、自己の秘密鍵を記憶しており、情報サーバから伝達された、暗号化された乱数を、当該秘密鍵で復号し、かつ情報サーバから伝達された、再暗号化された情報を、復号して得た乱数で復号する第2の復号手段を備えることを特徴としている。

【0022】上記のように、第4の発明では、乱数発生

手段が乱数を発生し、共通暗号化手段は、第1の復号手段が復号して得られた情報を、当該乱数で再暗号化する。また、データ記録手段が1以上の端末毎の秘密鍵を記憶しておき、共通暗号化手段は、さらに、乱数発生手段が発生した乱数を、当該秘密鍵で暗号化する。再暗号化された情報および暗号化された乱数が1以上の端末に伝達されると、第2の復号手段は、伝達された、暗号化された乱数を、記憶している自己の秘密鍵で復号し、さらに、伝達された、再暗号化された情報を、復号して得た乱数で復号する。このように、情報を乱数で再暗号化し、さらに、当該乱数を端末毎の秘密鍵で暗号化することにより、情報サーバから1以上の端末に、より安全に情報を伝達できる。

【0023】第5の発明は、1以上の情報提供者と契約者とからなり、情報提供者は、契約者に情報を提供し、契約者は、提供される情報を利用して、情報提供者に利用料金を支払うような情報提供システムの契約者側に設けられる情報サーバであって、1以上の情報提供者はそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信し、契約者側には、さらに、当該情報サーバに情報伝達可能に接続された1以上の端末が設けられており、1以上の情報提供者が提供する情報を受信する受信手段と、受信手段が受信した情報を記録する情報記録手段と、情報記録手段が記録した情報が、1以上の端末に伝達される毎に、当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定する課金手段と、課金手段が算定して得られた利用料金を記録するデータ記録手段とを備えている。

【0024】上記のように、第5の発明では、1以上の情報提供者は、提供しようとする情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する。契約者側には、情報サーバに情報伝達可能に接続された1以上の端末が、さらに設けられている。情報サーバの受信手段は、1以上の情報提供者が提供する情報を受信する。情報記録手段は、受信手段が受信した情報を記録する。課金手段は、情報記録手段が記録した情報が、1以上の端末に伝達される毎に、当該情報に付加された課金基準データに基づいて、当該情報の利用料金を算定する。データ記録手段は、課金手段が算定して得られた利用料金を記録する。なお、記録された利用料金は、所定の方法で各情報提供者に通知され、契約者は当該料金を支払うことになる。

【0025】このように、情報サーバは、1以上の情報提供者が提供する情報を記録する。そして、情報サーバは、記録した情報が1以上の端末に伝達される毎に、当該情報の利用料金を算定し、算定して得た利用料金を記録する。これにより、契約者が情報を記録して繰り返し利用する場合、利用度合に応じた課金ができる。

【0026】第6の発明は、第5の発明において、1以

上の情報提供者が提供する情報は、それぞれ暗号化されており、情報記録手段が記録した情報を復号する復号手段をさらに備えることを特徴としている。

【0027】上記のように、第6の発明では、1以上の情報提供者が提供する情報が暗号化されている場合、情報記録手段は、当該情報を暗号化されたままで記録する。復号手段は、情報記録手段が記録した情報が1以上の端末に伝達される際に、当該情報を復号する。

【0028】このように、提供される情報が暗号化されている場合、当該情報を暗号化されたままで記録し、当該情報が端末に伝達される際に復号することにより、記録された情報が不正に利用されるのを防ぐことができる。

【0029】第7の発明は、第6の発明において、1以上の端末はそれぞれ、自己の秘密鍵を記憶しており、情報サーバから伝達された、再暗号化された情報を、当該秘密鍵で復号する機能を有し、データ記録手段は、1以上の端末毎の秘密鍵を記憶しており、復号手段が復号して得られた情報を、データ記録手段が記憶している1以上の端末毎の秘密鍵でそれぞれ再暗号化する共通暗号化手段をさらに備えることを特徴としている。

【0030】上記のように、第7の発明では、データ記録手段が1以上の端末毎の秘密鍵を記憶しておき、共通暗号化手段は、復号手段が復号して得られた情報を、当該秘密鍵で再暗号化する。再暗号化された情報が1以上の端末に伝達されると、1以上の端末はそれぞれ、伝達された、再暗号化された情報を、記憶している自己の秘密鍵で復号する。これにより、情報サーバから1以上の端末に、安全に情報を伝達できる。

【0031】第8の発明は、第6の発明において、1以上の端末はそれぞれ、自己の秘密鍵を記憶しており、情報サーバから伝達された、暗号化された乱数を、当該秘密鍵で復号し、かつ、情報サーバから伝達された、再暗号化された情報を、復号して得た乱数で復号する機能を有し、データ記録手段は、1以上の端末毎の秘密鍵を記憶しており、乱数を発生する乱数発生手段と、復号手段が復号して得られた情報を、乱数発生手段が発生する乱数で再暗号化し、かつ、当該乱数を、データ記録手段が記憶している1以上の端末毎の秘密鍵で暗号化する共通暗号化手段とをさらに備えることを特徴としている。

【0032】上記のように、第8の発明では、乱数発生手段が乱数を発生し、共通暗号化手段は、復号手段が復号して得られた情報を、当該乱数で再暗号化する。また、データ記録手段が1以上の端末毎の秘密鍵を記憶しておき、共通暗号化手段は、さらに、乱数発生手段が発生した乱数を、当該秘密鍵で暗号化する。再暗号化された情報および暗号化された乱数が1以上の端末に伝達されると、1以上の端末はそれぞれ、伝達された、暗号化された乱数を、記憶している自己の秘密鍵で復号し、さらに、伝達された、再暗号化された情報を、復号して得

た乱数で復号する。このように、情報を乱数で再暗号化し、さらに、当該乱数を端末毎の秘密鍵で暗号化することにより、情報サーバから1以上の端末に、より安全に情報を伝達できる。

【0033】第9の発明は、1以上の情報提供者と契約者とからなり、情報提供者は、契約者に情報を提供し、契約者は、提供される情報を利用して、情報提供者に利用料金を支払うような情報提供システムの契約者側に設けられる端末であって、1以上の情報提供者はそれぞれ、提供すべき情報を暗号化したうえ、当該情報の利用料金を算定するための課金基準データを付加して配信し、契約者側には、端末の秘密鍵を記憶しており、1以上の情報提供者が提供する情報を受信し、かつ受信した情報を記録し、かつ記録した情報が端末に伝達される毎に、当該情報に付加されている課金基準データに基づいて当該情報の利用料金を算定し、かつ算定して得た利用料金を記録し、かつ記録した情報を復号し、かつ復号して得た情報を当該秘密鍵で再暗号化する機能を有する情報サーバがさらに設けられ、自己の秘密鍵を記憶しており、情報サーバから伝達された、再暗号化された情報を、当該秘密鍵で復号する復号手段を備えている。

【0034】上記のように、第9の発明では、1以上の情報提供者は、提供しようとする情報を暗号化したうえ、当該情報の利用料金を算定するための課金基準データを付加して配信する。契約者側に設けられた情報サーバは、1以上の情報提供者が提供する情報を受信して記録する。記録した情報が端末に伝達される毎に、情報サーバは、当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定し、算定して得た利用料金を記録する。なお、記録された利用料金は、所定の方法で各情報提供者に通知され、契約者は当該料金を支払うことになる。情報サーバは、端末毎の秘密鍵を記憶しておき、記録した情報が端末に伝達される際に、当該情報を復号し、復号して得た情報を、当該秘密鍵で再暗号化する。再暗号化された情報が端末に伝達されると、復号手段は、伝達された、再暗号化された情報を、記憶している自己の秘密鍵で復号する。

【0035】このように、情報サーバは、情報提供者が提供する情報を記録し、記録した情報が1以上の端末に伝達される毎に、その情報の利用料金を算定し、算定して得た利用料金を記録することにより、契約者が情報を記録して繰り返し利用する場合、利用度合に応じた課金を行う。記録した情報が端末に伝達される際に、情報サーバは、当該情報を復号し、復号して得た情報を、端末の秘密鍵で再暗号化する。端末は、伝達された、再暗号化された情報を復号する。これにより、利用度合に応じた課金を行う際、情報サーバから端末に、安全に情報を伝達することができる。

【0036】第10の発明は、1以上の情報提供者と契約者とからなり、情報提供者は、契約者に情報を提供

し、契約者は、提供される情報を利用して、情報提供者に利用料金を支払うような情報提供システムの契約者側に設けられる端末であって、1以上の情報提供者はそれぞれ、提供すべき情報を暗号化したうえ、当該情報の利用料金を算定するための課金基準データを付加して配信し、契約者側には、端末の秘密鍵を記憶しており、1以上の情報提供者が提供する情報を受信し、かつ受信した情報を記録し、かつ記録した情報が端末に伝達される毎に、当該情報に付加されている課金基準データに基づいて当該情報の利用料金を算定し、かつ算定して得た利用料金を記録し、かつ記録した情報を復号し、かつ乱数を発生し、かつ復号して得た情報を当該乱数で再暗号化し、かつ当該乱数を当該秘密鍵で暗号化する機能を有する情報サーバがさらに設けられ、自己の秘密鍵を記憶しており、情報サーバから伝達された、暗号化された乱数を、当該秘密鍵で復号し、かつ情報サーバから伝達された、再暗号化された情報を、復号して得た乱数で復号する復号手段を備えている。

【0037】上記のように、第10の発明では、1以上の情報提供者は、提供しようとする情報を暗号化したうえ、当該情報の利用料金を算定するための課金基準データを付加して配信する。契約者側に設けられた情報サーバは、1以上の情報提供者が提供する情報を受信して記録する。記録した情報が端末に伝達される毎に、情報サーバは、当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定し、算定して得た利用料金を記録する。なお、記録された利用料金は、所定の方法で各情報提供者に通知され、契約者は当該料金を支払うことになる。情報サーバは、記録した情報が端末に伝達される際に、当該情報を復号し、乱数を発生し、復号して得た情報を、当該乱数で再暗号化する。情報サーバはまた、端末の秘密鍵を記憶しておき、発生した乱数を、当該秘密鍵で暗号化する。再暗号化された情報および暗号化された乱数が端末に伝達されると、復号手段は、伝達された、暗号化された乱数を、記憶している自己の秘密鍵で復号し、さらに、伝達された、再暗号化された情報を、復号して得た乱数で復号する。

【0038】このように、情報サーバは、情報提供者が提供する情報を記録し、記録した情報が1以上の端末に伝達される毎に、その情報の利用料金を算定し、算定して得た利用料金を記録することにより、契約者が情報を記録して繰り返し利用する場合、利用度合に応じた課金を行う。記録した情報が端末に伝達される際に、情報サーバは、当該情報を復号し、乱数を発生し、復号して得た情報を、当該乱数で再暗号化し、さらに、当該乱数を、端末の秘密鍵で暗号化する。端末は、伝達された、暗号化された乱数を、自己の秘密鍵で復号し、さらに、伝達された、再暗号化された情報を、復号して得た乱数で復号する。これにより、利用度合に応じた課金を行う際、情報サーバから端末に、安全に情報を伝達すること

ができる。

【0039】第11の発明は、1以上の情報提供者と契約者とからなり、情報提供者は、契約者に情報を提供し、契約者は、提供される情報を利用して、情報提供者に利用料金を支払うような情報提供システムであって、1以上の情報提供者側にはそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する配信手段が設けられ、契約者側には、情報サーバおよびオフライン端末が設けられ、情報サーバは、1以上の情報提供者が提供する情報を受信する受信手段と、受信手段が受信した情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成し、かつ、作成した実行権データおよび当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定する課金手段と、課金手段が算定して得られた利用料金を記録するデータ記録手段とを備え、オフライン端末は、情報サーバから伝達された実行権データが所定の条件を満たす場合に、情報サーバから伝達された情報の利用を許可することを特徴としている。

【0040】上記のように、第11の発明では、1以上の情報提供者側に設けられた配信手段はそれぞれ、提供しようとする情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する。契約者側には、情報サーバおよびオフライン端末が設けられ、情報サーバの受信手段は、1以上の情報提供者が提供する情報を受信する。課金手段は、受信手段が受信した情報の利用度合および当該情報を利用できる端末を制限するための実行権データを作成し、かつ作成した実行権データおよび当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定する。データ記録手段は、課金手段が算定して得られた利用料金を記録する。なお、記録された利用料金は、所定の方法で各情報提供者に通知され、契約者は当該料金を支払うことになる。受信手段が受信した情報および課金手段が作成した実行権データがオフライン端末に伝達されると、オフライン端末は、伝達された実行権データが所定の条件を満たす場合に、伝達された情報の利用を許可する。

【0041】このように、情報サーバは、情報の利用度合および情報を利用できる端末を制限するための実行権データを作成し、同時に、当該情報に付加された課金基準データを参照して、作成した実行権データに応じた利用料金を算定して記録する。オフライン端末は、伝達された実行権データが所定の条件を満たす場合に、伝達された情報を利用するのを許可する。これにより、契約者がオフライン端末において情報を利用する場合、利用度合に応じた課金ができる。

【0042】第12の発明は、第11の発明において、1以上の情報提供者が提供する情報は、それぞれ暗号化されており、情報サーバは、受信手段が受信した情報を

復号する第1の復号手段をさらに備えることを特徴としている。

【0043】これにより、1以上の情報提供者が提供する情報が暗号化されている場合、情報サーバは、当該情報を復号できる。

【0044】第13の発明は、第12の発明において、情報サーバは、第1の復号手段が復号して得られた情報を、所定の方式で再暗号化する共通暗号化手段をさらに備え、オフライン端末は、情報サーバから伝達された、再暗号化された情報を、情報サーバから伝達された実行権データが所定の条件を満たす場合に復号する第2の復号手段を備えることを特徴としている。

【0045】これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0046】第14の発明は、第12の発明において、情報サーバは、乱数を発生する乱数発生手段と、第1の復号手段が復号して得られた情報を、乱数発生手段が発生する乱数で再暗号化する共通暗号化手段とをさらに備え、オフライン端末は、情報サーバから伝達された、再暗号化された情報を、情報サーバから伝達された実行権データが所定の条件を満たす場合に、情報サーバから伝達された乱数で復号する第2の復号手段を備えることを特徴としている。

【0047】上記のように、第14の発明では、乱数発生手段が乱数を発生し、共通暗号化手段は、第1の復号手段が復号して得られた情報を、当該乱数で再暗号化する。再暗号化された情報、発生された乱数および作成された実行権データがオフライン端末に伝達されると、第2の復号手段は、伝達された、再暗号化された情報を、伝達された実行権データが所定の条件を満たす場合に、伝達された乱数で復号する。これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0048】第15の発明は、第14の発明において、共通暗号化手段が再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、乱数発生手段が発生した乱数および課金手段が作成した実行権データは、記録内容の解析／変更が困難な携帯型記録媒体を介して、それぞれオフライン端末に伝達されることを特徴としている。

【0049】これにより、情報サーバからオフライン端末に、安全に情報を伝達できる。

【0050】第16の発明は、1以上の情報提供者と契約者とからなり、情報提供者は、契約者に情報を提供し、契約者は、提供される情報を利用して、情報提供者に利用料金を支払うような情報提供システムの契約者側に設けられる情報サーバであって、1以上の情報提供者はそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信し、契約

者側には、さらに、伝達された実行権データが所定の条件を満たす場合に、伝達された情報の利用を許可する機能を有するオフライン端末が設けられ、1以上の情報提供者が提供する情報を受信する受信手段と、受信手段が受信した情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成し、かつ、作成した実行権データおよび当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定する課金手段と、課金手段が算定して得られた利用料金を記録するデータ記録手段とを備えている。

【0051】上記のように、第16の発明では、1以上の情報提供者はそれぞれ、提供しようとする情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する。受信手段は、1以上の情報提供者が提供する情報を受信する。課金手段は、受信手段が受信した情報の利用度合および当該情報を利用できる端末を制限するための実行権データを作成し、かつ作成した実行権データおよび当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定する。データ記録手段は、課金手段が算定して得られた利用料金を記録する。なお、記録された利用料金は、所定の方法で各情報提供者に通知され、契約者は当該料金を支払うことになる。受信手段が受信した情報および課金手段が作成した実行権データがオフライン端末に伝達されると、オフライン端末は、伝達された実行権データが所定の条件を満たす場合に、伝達された情報の利用を許可する。

【0052】このように、情報サーバは、情報の利用度合および当該情報を利用できる端末を制限するための実行権データを作成し、同時に、当該情報に付加された課金基準データを参照して、作成した実行権データに応じた利用料金を算定して記録する。オフライン端末は、伝達された実行権データが所定の条件を満たす場合に、情報を利用するのを許可する。これにより、契約者がオフライン端末において情報を利用する場合、利用度合に応じた課金ができる。

【0053】第17の発明は、第16の発明において、1以上の情報提供者が提供する情報は、それぞれ暗号化されており、受信手段が受信した情報を復号する復号手段をさらに備えることを特徴としている。

【0054】これにより、1以上の情報提供者が提供する情報が暗号化されている場合、当該情報を復号できる。

【0055】第18の発明は、第17の発明において、オフライン端末は、情報サーバから伝達された、再暗号化された情報を、情報サーバから伝達された実行権データが所定の条件を満たす場合に復号する機能を有しており、復号手段が復号して得られた情報を、所定的方式で再暗号化する共通暗号化手段をさらに備えることを特徴としている。

【0056】これにより、実行権データが所定の条件を

満たす場合にのみ、情報を利用可能にすることができる。

【0057】第19の発明は、第17の発明において、オフライン端末は、情報サーバから伝達された、再暗号化された情報を、情報サーバから伝達された実行権データが所定の条件を満たす場合に、情報サーバから伝達された乱数で復号する機能を有しており、乱数を発生する乱数発生手段と、復号手段が復号して得られた情報を、乱数発生手段が発生する乱数で再暗号化する共通暗号化手段とをさらに備えることを特徴としている。

【0058】上記のように、第19の発明では、乱数発生手段が乱数を発生し、共通暗号化手段は、復号手段が復号して得られた情報を、当該乱数で再暗号化する。再暗号化された情報、発生された乱数および作成された実行権データがオフライン端末に伝達されると、オフライン端末は、伝達された、再暗号化された情報を、伝達された実行権データが所定の条件を満たす場合に、伝達された乱数で復号する。これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0059】第20の発明は、第19の発明において、共通暗号化手段が再暗号化して得られた情報は、書き込み/読み出し可能な携帯型記録媒体を介して、乱数発生手段が発生した乱数および課金手段が作成した実行権データは、記録内容の解析/変更が困難な携帯型記録媒体を介して、それぞれオフライン端末に伝達されることを特徴としている。

【0060】これにより、情報サーバからオフライン端末に、安全に情報を伝達できる。

【0061】第21の発明は、1以上の情報提供者と契約者とからなり、情報提供者は、契約者に情報を提供し、契約者は、提供される情報を利用して、情報提供者に利用料金を支払うような情報提供システムの契約者側に設けられるオフライン端末であって、1以上の情報提供者はそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信し、契約者側には、さらに、1以上の情報提供者が提供する情報を受信し、かつ受信した情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成し、かつ作成した実行権データおよび当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定し、かつ算定して得た利用料金を記録する機能を有する情報サーバが設けられ、情報サーバから伝達された実行権データが所定の条件を満たす場合に、情報サーバから伝達された情報の利用を許可することを特徴としている。

【0062】上記のように、第21の発明では、1以上の情報提供者はそれぞれ、提供しようとする情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する。契約者側に設けられた情報サーバは、

各情報提供者が提供する情報を受信すると、受信した情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成し、かつ作成した実行権データおよび当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定して記録する。再暗号化された情報および作成された実行権データがオフライン端末に伝達されると、オフライン端末は、伝達された実行権データが所定の条件を満たす場合に、伝達された情報の利用を許可する。

【0063】このように、情報サーバは、情報の利用度合および情報を利用できる端末を制限するための実行権データを作成し、同時に、当該情報に付加された課金基準データを参照して、作成した実行権データに応じた利用料金を算定して記録する。オフライン端末は、伝達された実行権データが所定の条件を満たす場合に、伝達された情報の利用を許可する。これにより、契約者がオフライン端末で情報を利用する場合、利用度合に応じて課金できる。

【0064】第22の発明は、第21の発明において、1以上の情報提供者が提供する情報は、それぞれ暗号化されており、情報サーバは、受信した情報を復号する機能をさらに有することを特徴としている。

【0065】これにより、1以上の情報提供者が提供する情報が暗号化されている場合、情報サーバは、当該情報を復号できる。

【0066】第23の発明は、第22の発明において、情報サーバは、復号して得た情報を、所定の方式で再暗号化する機能をさらに有し、情報サーバから伝達された、再暗号化された情報を、情報サーバから伝達された実行権データが所定の条件を満たす場合に復号する復号手段を備えることを特徴としている。

【0067】これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0068】第24の発明は、第22の発明において、情報サーバは、乱数を発生し、かつ、復号して得た情報を、当該乱数で再暗号化する機能をさらに有し、情報サーバから伝達された、再暗号化された情報を、情報サーバから伝達された実行権データが所定の条件を満たす場合に、情報サーバから伝達された乱数で復号する復号手段を備えることを特徴としている。

【0069】上記のように、第24の発明では、情報サーバは、乱数を発生し、復号して得た情報を、当該乱数で再暗号化する。再暗号化された情報、発生された乱数および作成された実行権データがオフライン端末に伝達されると、復号手段は、伝達された、暗号化された乱数および実行権データを復号し、さらに、伝達された、再暗号化された情報を、復号して得た実行権データが所定の条件を満たす場合に、復号して得た乱数で復号する。これにより、実行権データが所定の条件を満たす場合に

のみ、情報を利用可能にすることができる。

【0070】第25の発明は、第24の発明において、情報サーバが再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、情報サーバが発生した乱数および作成した実行権データは、記録内容の解析／変更が困難な携帯型記録媒体を介して、それぞれオフライン端末に伝達されることを特徴としている。

【0071】これにより、情報サーバからオフライン端末に、安全に情報を伝達できる。

10 【0072】第26の発明は、1以上の情報提供者と第1および第2の契約者とからなり、情報提供者は、第1の契約者に情報を提供し、第1の契約者は、提供される情報を第2の契約者に再提供して、第1の契約者が情報提供者に利用料金を支払うような情報提供システムであって、1以上の情報提供者側にはそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する配信手段が設けられ、第1の契約者側には情報サーバが、第2の契約者側には1以上の端末がそれぞれ設けられ、情報サーバは、1以上の情報提供者が提供する情報を受信する受信手段と、受信手段が受信した情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成し、かつ、作成した実行権データおよび当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定する課金手段と、課金手段が算定して得られた利用料金を記録するデータ記録手段とを備え、1以上の端末はそれぞれ、情報サーバから伝達された実行権データが所定の条件を満たす場合に、情報サーバから伝達された情報の利用を許可することを特徴としている。

30 【0073】上記のように、第26の発明では、1以上の情報提供者側に設けられた配信手段はそれぞれ、提供しようとする情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する。第1の契約者側には情報サーバが、第2の契約者側には1以上の端末がそれぞれ設けられており、情報サーバの受信手段は、1以上の情報提供者が提供する情報を受信する。課金手段は、受信手段が受信した情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成し、かつ作成した実行権データおよび当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定する。データ記録手段は、課金手段が算定して得られた利用料金を記録する。なお、記録された利用料金は、所定の方法で各情報提供者に通知され、契約者は当該料金を支払うことになる。受信手段が受信した情報および課金手段が作成した実行権データが第2の契約者側に伝達されると、1以上の端末はそれぞれ、伝達された実行権データが所定の条件を満たす場合に、伝達された情報の利用を許可する。

50 【0074】このように、第1の契約者側に設けられた情報サーバは、情報の利用度合および情報を利用できる

端末を制限するための実行権データを作成し、同時に、当該情報に付加された課金基準データを参照して、作成した実行権データに応じた利用料金を算定して記録する。一方、第2の契約者側に設けられた1以上の端末はそれぞれ、伝達された実行権データが所定の条件を満たす場合に、伝達された情報を利用するのを許可する。これにより、第1の契約者が受信した情報を第2の契約者が利用する場合、利用度合に応じて、第1の契約者に課金できる。なお、第1の契約者により受信された情報を第2の契約者が利用して、第1の契約者に課金するという提供形態は、情報をプレゼントするという、情報提供の新たな形態である。

【0075】第27の発明は、第26の発明において、1以上の情報提供者が提供する情報は、それぞれ暗号化されており、情報サーバは、受信手段が受信した情報を復号する第1の復号手段をさらに備えることを特徴としている。

【0076】これにより、1以上の情報提供者が提供する情報が暗号化されている場合、情報サーバは、当該情報を復号できる。

【0077】第28の発明は、第27の発明において、情報サーバは、第1の復号手段が復号して得られた情報を、所定の方式で再暗号化する共通暗号化手段をさらに備え、1以上の端末はそれぞれ、情報サーバから伝達された、再暗号化された情報を、情報サーバから伝達された実行権データが所定の条件を満たす場合に復号する第2の復号手段を備えることを特徴としている。

【0078】これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0079】第29の発明は、第27の発明において、情報サーバは、乱数を発生する乱数発生手段と、第1の復号手段が復号して得られた情報を、乱数発生手段が発生する乱数で再暗号化する共通暗号化手段とをさらに備え、1以上の端末はそれぞれ、情報サーバから伝達された、再暗号化された情報を、情報サーバから伝達された実行権データが所定の条件を満たす場合に、情報サーバから伝達された乱数で復号する第2の復号手段を備えることを特徴としている。

【0080】上記のように、第29の発明では、乱数発生手段が乱数を発生し、共通暗号化手段は、第1の復号手段が復号して得られた情報を、当該乱数で再暗号化する。再暗号化された情報、発生された乱数および作成された実行権データが第2の契約者側に伝達されると、第2の復号手段は、伝達された、再暗号化された情報を、伝達された実行権データが所定の条件を満たす場合に、伝達された乱数で復号する。これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0081】第30の発明は、第29の発明において、

共通暗号化手段が再暗号化して得られた情報は、書き込み/読み出し可能な携帯型記録媒体を介して、乱数発生手段が発生した乱数および課金手段が作成した実行権データは、記録内容の解析/変更が困難な携帯型記録媒体を介して、それぞれ第2の契約者側に伝達されることを特徴としている。

【0082】これにより、第1の契約者側から第2の契約者側に、安全に情報を伝達できる。

【0083】第31の発明は、第27の発明において、情報サーバは、乱数を発生する乱数発生手段と、第1の復号手段が復号して得られた情報を、乱数発生手段が発生する乱数で再暗号化し、かつ、乱数発生手段が発生した乱数および課金手段が作成した実行権データを所定の方式で暗号化する共通暗号化手段とをさらに備え、1以上の端末はそれぞれ、情報サーバから伝達された、暗号化された乱数および実行権データを復号し、かつ、情報サーバから伝達された、再暗号化された情報を、復号して得た実行権データが所定の条件を満たす場合に、復号して得た乱数で復号する第2の復号手段を備えることを特徴としている。

【0084】上記のように、第31の発明では、乱数発生手段が乱数を発生し、共通暗号化手段は、第1の復号手段が復号して得られた情報を、当該乱数で再暗号化し、さらに、当該乱数および課金手段が作成した実行権データを所定の方式で暗号化する。再暗号化された情報ならびに暗号化された乱数および実行権データが第2の契約者側に伝達されると、第2の復号手段は、伝達された、暗号化された乱数および実行権データを復号し、さらに、伝達された、再暗号化された情報を、復号して得た実行権データが所定の条件を満たす場合に、復号して得た乱数で復号する。これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0085】第32の発明は、第31の発明において、共通暗号化手段が再暗号化して得られた情報ならびに共通暗号化手段が暗号化して得られた乱数および実行権データは、伝送速度が比較的大きい伝送路を介して、第2の契約者側に伝達されることを特徴としている。

【0086】第33の発明は、第31の発明において、共通暗号化手段が再暗号化して得られた情報は、書き込み/読み出し可能な携帯型記録媒体を介して、共通暗号化手段が暗号化して得られた乱数および実行権データは、伝送速度が比較的小さい伝送路を介して、それぞれ第2の契約者側に伝達されることを特徴としている。

【0087】第32および第33の発明により、第1の契約者側から第2の契約者側に、安全に情報を伝達できる。

【0088】第34の発明は、1以上の情報提供者と第1および第2の契約者とからなり、情報提供者は、第1の契約者に情報を提供し、第1の契約者は、提供される

情報を第2の契約者に再提供して、第1の契約者が情報提供者に利用料金を支払うような情報提供システムの第1の契約者側に設けられる情報サーバであって、1以上の情報提供者はそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信し、第2の契約者側には、情報サーバから伝達された実行権データが所定の条件を満たす場合に、情報サーバから伝達された情報の利用を許可する機能を有する1以上の端末が設けられており、1以上の情報提供者が提供する情報を受信する受信手段と、受信手段が受信した情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成し、かつ、作成した実行権データおよび当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定する課金手段と、課金手段が算定して得られた利用料金を記録するデータ記録手段とを備えている。

【0089】上記のように、第34の発明では、1以上の情報提供者はそれぞれ、提供しようとする情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する。受信手段は、1以上の情報提供者が提供する情報を受信する。課金手段は、受信手段が受信した情報の利用度合および当該情報を利用できる端末を制限するための実行権データを作成し、かつ作成した実行権データおよび当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定する。データ記録手段は、課金手段が算定して得られた利用料金を記録する。なお、記録された利用料金は、所定の方法で各情報提供者に通知され、契約者は当該料金を支払うことになる。受信手段が受信した情報および課金手段が作成した実行権データが第2の契約者側に伝達されると、1以上の端末はそれぞれ、伝達された実行権データが所定の条件を満たす場合に、伝達された情報の利用を許可する。

【0090】このように、第1の契約者側に設けられた情報サーバは、情報の利用度合および情報を利用できる端末を制限するための実行権データを作成し、同時に、当該情報に付加された課金基準データを参照して、作成した実行権データに応じた利用料金を算定して記録する。一方、第2の契約者側に設けられた1以上の端末はそれぞれ、伝達された実行権データが所定の条件を満たす場合に、伝達された情報を利用するのを許可する。これにより、第1の契約者が受信した情報を、第2の契約者が利用する場合、利用度合に応じて、第1の契約者に課金できる。なお、第1の契約者により受信された情報を第2の契約者が利用して、第1の契約者に課金するという提供形態は、情報をプレゼントするという、情報提供の新たな形態である。

【0091】第35の発明は、第34の発明において、1以上の情報提供者が提供する情報は、それぞれ暗号化されており、受信手段が受信した情報を復号する復号手

段をさらに備えることを特徴としている。

【0092】これにより、1以上の情報提供者が提供する情報が暗号化されている場合、当該情報を復号できる。

【0093】第36の発明は、第35の発明において、1以上の端末はそれぞれ、情報サーバから伝達された、再暗号化された情報を、情報サーバから伝達された実行権データが所定の条件を満たす場合に復号する機能を有しており、復号手段が復号して得られた情報を、所定の方式で再暗号化する共通暗号化手段をさらに備えることを特徴としている。

【0094】これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0095】第37の発明は、第35の発明において、1以上の端末はそれぞれ、情報サーバから伝達された、再暗号化された情報を、情報サーバから伝達された実行権データが所定の条件を満たす場合に、情報サーバから伝達された乱数で復号する機能を有しており、乱数を発生する乱数発生手段と、復号手段が復号して得られた情報を、乱数発生手段が発生する乱数で再暗号化する共通暗号化手段とをさらに備えることを特徴としている。

【0096】上記のように、第37の発明では、乱数発生手段が乱数を発生し、共通暗号化手段は、復号手段が復号して得られた情報を、当該乱数で再暗号化する。再暗号化された情報、発生された乱数および作成された実行権データが第2の契約者側に伝達されると、1以上の端末はそれぞれ、伝達された、再暗号化された情報を、伝達された実行権データが所定の条件を満たす場合に、伝達された乱数で復号する。これにより、伝達された実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0097】第38の発明は、第37の発明において、共通暗号化手段が再暗号化して得られた情報は、書き込み/読み出し可能な携帯型記録媒体を介して、乱数発生手段が発生した乱数および課金手段が作成した実行権データは、記録内容の解析/変更が困難な携帯型記録媒体を介して、それぞれ第2の契約者側に伝達されることを特徴としている。

【0098】これにより、第1の契約者側から第2の契約者側に、安全に情報を伝達できる。

【0099】第39の発明は、第35の発明において、1以上の端末はそれぞれ、情報サーバから伝達された、暗号化された乱数および実行権データを復号し、かつ、情報サーバから伝達された、再暗号化された情報を、復号して得た実行権データが所定の条件を満たす場合に、復号して得た乱数で復号する機能を有しており、乱数を発生する乱数発生手段と、復号手段が復号して得られた情報を、乱数発生手段が発生する乱数で再暗号化し、かつ、乱数発生手段が発生した乱数および課金手段が作成

した実行権データを所定の方式で暗号化する共通暗号化手段とをさらに備えることを特徴としている。

【0100】上記のように、第39の発明では、乱数発生手段が乱数を発生し、共通暗号化手段は、復号手段が復号して得られた情報を当該乱数で再暗号化し、かつ当該乱数および課金手段が作成した実行権データを所定の方式で暗号化する。再暗号化された情報ならびに暗号化された乱数および実行権データが第2の契約者側に伝達されると、1以上の端末はそれぞれ、伝達された、暗号化された乱数および実行権データを復号し、さらに、伝達された、再暗号化された情報を、復号して得た実行権データが所定の条件を満たす場合に、復号して得た乱数で復号する。これにより、伝達された実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0101】第40の発明は、第39の発明において、共通暗号化手段が再暗号化して得られた情報ならびに共通暗号化手段が暗号化して得られた乱数および実行権データは、伝送速度が比較的大きい伝送路を介して、第2の契約者側に伝達されることを特徴としている。

【0102】第41の発明は、第39の発明において、共通暗号化手段が再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、共通暗号化手段が暗号化して得られた乱数および実行権データは、伝送速度が比較的小さい伝送路を介して、それぞれ第2の契約者側に伝達されることを特徴としている。

【0103】第40および第41の発明により、第1の契約者側から第2の契約者側に、安全に情報を伝達できる。

【0104】第42の発明は、1以上の情報提供者と第1および第2の契約者とからなり、情報提供者は、第1の契約者に情報を提供し、第1の契約者は、提供される情報を第2の契約者に再提供して、第1の契約者が情報提供者に利用料金を支払うような情報提供システムの第2の契約者側に設けられる端末であって、1以上の情報提供者はそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信し、第1の契約者側には、1以上の情報提供者が提供する情報を受信し、かつ受信した情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成し、かつ作成した実行権データおよび当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定し、かつ算定して得た利用料金を記録する機能を有する情報サーバが設けられ、情報サーバから伝達された実行権データが所定の条件を満たす場合に、情報サーバから伝達された情報の利用を許可することを特徴としている。

【0105】上記のように、第42の発明では、1以上の情報提供者はそれぞれ、提供しようとする情報に、当該情報の利用料金を算定するための課金基準データを付

加して配信する。第1の契約者側に設けられた情報サーバは、1以上の情報提供者が提供する情報を受信すると、当該情報の利用度合および当該情報を利用できる端末を制限するための実行権データを作成し、かつ作成した実行権データおよび当該情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定して記録する。情報サーバが受信した情報および作成した実行権データが第2の契約者側に伝達されると、端末は、伝達された実行権データが所定の条件を満たす場合に、伝達された情報を利用するのを許可する。

【0106】このように、第1の契約者側に設けられた情報サーバは、情報の利用度合および情報を利用できる端末を制限するための実行権データを作成し、同時に、当該情報に付加された課金基準データを参照して、作成した実行権データに応じた利用料金を算定して記録する。一方、第2の契約者側に設けられた端末は、伝達された実行権データが所定の条件を満たす場合に、伝達された情報を利用するのを許可する。これにより、第1の契約者が受信した情報を、第2の契約者が利用する場合、利用度合に応じて、第1の契約者に課金できる。

【0107】第43の発明は、第42の発明において、1以上の情報提供者が提供する情報は、それぞれ暗号化されており、情報サーバは、受信した情報を復号する機能をさらに有することを特徴としている。

【0108】これにより、1以上の情報提供者が提供する情報が暗号化されている場合、情報サーバは、当該情報を復号できる。

【0109】第44の発明は、第43の発明において、情報サーバは、復号して得た情報を所定の方式で再暗号化する機能をさらに有し、情報サーバから伝達された、再暗号化された情報を、情報サーバから伝達された実行権データが所定の条件を満たす場合に復号する復号手段を備えることを特徴としている。

【0110】これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0111】第45の発明は、第43の発明において、情報サーバは、乱数を発生し、かつ復号して得た情報を当該乱数で再暗号化する機能をさらに有し、情報サーバから伝達された、再暗号化された情報を、情報サーバから伝達された実行権データが所定の条件を満たす場合に、情報サーバから伝達された乱数で復号する復号手段を備えることを特徴としている。

【0112】上記のように、第45の発明では、情報サーバは、乱数を発生し、復号して得た情報を、当該乱数で再暗号化する。再暗号化された情報、発生された乱数および作成された実行権データが第2の契約者側に伝達されると、復号手段は、伝達された、再暗号化された情報を、伝達された実行権データが所定の条件を満たす場合に、伝達された乱数で復号する。これにより、実行権

データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0113】第46の発明は、第45の発明において、情報サーバが再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、情報サーバが発生した乱数および作成した実行権データは、記録内容の解析／変更が困難な携帯型記録媒体を介して、それぞれ第2の契約者側に伝達されることを特徴としている。

【0114】これにより、第1の契約者側から第2の契約者側に、安全に情報を伝達できる。

【0115】第47の発明は、第43の発明において、情報サーバは、乱数を発生し、かつ復号して得た情報を当該乱数で再暗号化し、かつ当該乱数および作成した実行権データを所定の方式で暗号化する機能をさらに有し、情報サーバから伝達された、暗号化された乱数および実行権データを復号し、かつ、情報サーバから伝達された、再暗号化された情報を、復号して得た実行権データが所定の条件を満たす場合に、復号して得た乱数で復号する復号手段を備えることを特徴としている。

【0116】上記のように、第47の発明では、情報サーバは、乱数を発生し、復号して得た情報を、当該乱数で再暗号化し、かつ当該乱数および作成した実行権データを所定の方式で暗号化する。再暗号化された情報ならびに暗号化された乱数および実行権データが第2の契約者側に伝達されると、復号手段は、伝達された、暗号化された乱数および実行権データを復号し、さらに、伝達された、再暗号化された情報を、復号して得た実行権データが所定の条件を満たす場合に、復号して得た乱数で復号する。これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0117】第48の発明は、第47の発明において、情報サーバが再暗号化して得られた情報ならびに情報サーバが暗号化して得られた乱数および実行権データは、伝送速度が比較的大きい伝送路を介して、第2の契約者側に伝達されることを特徴としている。

【0118】第49の発明は、第47の発明において、情報サーバが再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、情報サーバが暗号化して得られた乱数および実行権データは、伝送速度が比較的小さい伝送路を介して、それぞれ第2の契約者側に伝達されることを特徴としている。

【0119】第48および第49の発明により、第1の契約者側から第2の契約者側に、安全に情報を伝達できる。

【0120】第50の発明は、1以上の情報提供者と第1および第2の契約者とからなり、情報提供者は、第1の契約者に情報を提供し、第1の契約者は、提供される情報を第2の契約者に再提供して、第2の契約者が情報提供者に利用料金を支払うような情報提供システムであって、1以上の情報提供者側にはそれぞれ、提供すべき

情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する配信手段が設けられ、第1の契約者側には第1の情報サーバが、第2の契約者側には第2の情報サーバおよび当該情報サーバに情報伝達可能に接続された1以上の端末がそれぞれ設けられ、第1の情報サーバは、1以上の情報提供者が提供する情報を受信する受信手段と、受信手段が受信した情報を利用可能な端末を制限するための実行権データを作成する実行権データ作成手段とを備え、第2の情報サーバは、第1の情報サーバから伝達された情報に付加された課金基準データに基づいて、当該情報の利用料金を算定する課金手段と、課金手段が算定して得られた利用料金を記録するデータ記録手段とを備え、1以上の端末はそれぞれ、第1の情報サーバから伝達された実行権データが所定の条件を満たす場合に、第1の情報サーバから伝達された情報の利用を許可することを特徴としている。

【0121】上記のように、第50の発明では、1以上の情報提供者側に設けられた配信手段はそれぞれ、提供しようとする情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する。第1の契約者側には第1の情報サーバが、第2の契約者側には第2の情報サーバおよび当該情報サーバに情報伝達可能に接続された1以上の端末がそれぞれ設けられ、第1の情報サーバの受信手段は、1以上の情報提供者が提供する情報を受信する。実行権データ作成手段は、受信手段が受信した情報を利用可能な端末を制限するための実行権データを作成する。受信手段が受信した情報および実行権データ作成手段が作成した実行権データが、第2の契約者側に伝達されると、第2の情報サーバの課金手段は、伝達された情報に付加された課金基準データに基づいて、当該情報の利用料金を算定する。データ記録手段は、課金手段が算定して得られた利用料金を記録する。1以上の端末はそれぞれ、伝達された実行権データが所定の条件を満たす場合に、伝達された情報の利用を許可する。

【0122】このように、第1の契約者側に設けられた第1の情報サーバは、情報を利用できる端末を制限するための実行権データを作成する。一方、第2の契約者側に設けられた第2の情報サーバは、伝達された情報に付加された課金基準データを参照して、当該情報の利用料金を算定して記録する。1以上の端末はそれぞれ、伝達された実行権データが所定の条件を満たす場合に、伝達された情報の利用を許可する。これにより、第1の契約者が受信した情報を第2の契約者が利用する場合、利用度合に応じて、第2の契約者に課金できる。

【0123】第51の発明は、第50の発明において、1以上の情報提供者が提供する情報は、それぞれ暗号化されており、第1の情報サーバは、受信手段が受信した情報を復号する第1の復号手段をさらに備えることを特徴としている。

【0124】これにより、1以上の情報提供者が提供す

る情報が暗号化されている場合、第1の情報サーバは、当該情報を復号できる。

【0125】第52の発明は、第51の発明において、第1の情報サーバは、第1の復号手段が復号して得られた情報を、所定の方式で再暗号化する共通暗号化手段をさらに備え、1以上の端末はそれぞれ、第1の情報サーバから伝達された、再暗号化された情報を、第1の情報サーバから伝達された実行権データが所定の条件を満たす場合に復号する第2の復号手段を備えることを特徴としている。

【0126】これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0127】第53の発明は、第51の発明において、第1の情報サーバは、乱数を発生する乱数発生手段と、第1の復号手段が復号して得られた情報を、乱数発生手段が発生する乱数で再暗号化する共通暗号化手段とをさらに備え、1以上の端末はそれぞれ、第1の情報サーバから伝達された、再暗号化された情報を、第1の情報サーバから伝達された実行権データが所定の条件を満たす場合に、第1の情報サーバから伝達された乱数で復号する第2の復号手段を備えることを特徴としている。

【0128】上記のように、第53の発明では、第1の情報サーバの乱数発生手段は、乱数を発生する。共通暗号化手段は、第1の復号手段が復号して得られた情報を、乱数発生手段が発生する乱数で再暗号化する。再暗号化された情報、発生された乱数および作成された実行権データが第2の契約者側に伝達されると、1以上の端末の第2の復号手段は、伝達された、再暗号化された情報を、伝達された実行権データが所定の条件を満たす場合に、伝達された乱数で復号する。これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0129】第54の発明は、第53の発明において、共通暗号化手段が再暗号化して得られた情報は、書き込み/読み出し可能な携帯型記録媒体を介して、乱数発生手段が発生した乱数および課金手段が作成した実行権データは、記録内容の解析/変更が困難な携帯型記録媒体を介して、それぞれ第2の契約者側に伝達されることを特徴としている。

【0130】これにより、第1の契約者側から第2の契約者側に、安全に情報を伝達できる。

【0131】第55の発明は、第51の発明において、第1の情報サーバは、乱数を発生する乱数発生手段と、第1の復号手段が復号して得られた情報を、乱数発生手段が発生する乱数で再暗号化し、かつ、乱数発生手段が発生した乱数および実行権データ作成手段が作成した実行権データを所定の方式で暗号化する共通暗号化手段とをさらに備え、1以上の端末はそれぞれ、第1の情報サーバから伝達された、暗号化された乱数および実行権デ

ータを復号し、かつ、第1の情報サーバから伝達された、再暗号化された情報を、復号して得た実行権データが所定の条件を満たす場合に、復号して得た乱数で復号する第2の復号手段を備えることを特徴としている。

【0132】上記のように、第55の発明では、第1の情報サーバの乱数発生手段は、乱数を発生する。共通暗号化手段は、第1の復号手段が復号して得られた情報を乱数発生手段が発生する乱数で再暗号化し、かつ、当該乱数および実行権データ作成手段が作成した実行権データを所定の方式で暗号化する。再暗号化された情報ならびに暗号化された乱数および実行権データが第2の契約者側に伝達されると、1以上の端末の第2の復号手段は、伝達された、暗号化された乱数および実行権データを復号し、さらに、伝達された、再暗号化された情報を、復号して得た実行権データが所定の条件を満たす場合に、復号して得た乱数で復号する。これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0133】第56の発明は、第55の発明において、共通暗号化手段が再暗号化して得られた情報ならびに共通暗号化手段が暗号化して得られた乱数および実行権データは、伝送速度が比較的大きい伝送路を介して、第2の契約者側に伝達されることを特徴としている。

【0134】第57の発明は、第55の発明において、共通暗号化手段が再暗号化して得られた情報は、書き込み/読み出し可能な携帯型記録媒体を介して、共通暗号化手段が暗号化して得られた乱数および実行権データは、伝送速度が比較的小さい伝送路を介して、それぞれ第2の契約者側に伝達されることを特徴としている。

【0135】第56および第57の発明により、第1の契約者側から第2の契約者側に、安全に情報を伝達できる。

【0136】第58の発明は、1以上の情報提供者と第1および第2の契約者とからなり、情報提供者は、第1の契約者に情報を提供し、第1の契約者は、提供される情報を第2の契約者に再提供して、第2の契約者が情報提供者に利用料金を支払うような情報提供システムの第1の契約者側に設けられる情報サーバであって、1以上の情報提供者はそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信し、第2の契約者側には、伝達された情報に付加された課金基準データに基づいて、当該情報の利用料金を算定し、かつ算定して得た利用料金を記録する機能を有する他の情報サーバ、および当該他の情報サーバに情報伝達可能に接続され、情報サーバから伝達された実行権データが所定の条件を満たす場合に、情報サーバから伝達された情報の利用を許可する機能を有する1以上の端末が設けられており、1以上の情報提供者が提供する情報を受信する受信手段と、受信手段が受信した情報を利用可能な端末を制限するための実行権データを作成する

実行権データ作成手段とを備えている。

【0137】上記のように、第58の発明では、1以上の情報提供者はそれぞれ、提供しようとする情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する。受信手段は、1以上の情報提供者が提供する情報を受信する。実行権データ作成手段は、受信手段が受信した情報を利用可能な端末を制限するための実行権データを作成する。受信手段が受信した情報および実行権データ作成手段が作成した実行権データが第2の契約者側に伝達されると、他の情報サーバは、伝達された情報に付加された課金基準データに基づいて、当該情報の利用料金を算定し、かつ算定して得た利用料金を記録する。1以上の端末はそれぞれ、伝達された実行権データが所定の条件を満たす場合に、伝達された情報の利用を許可する。

【0138】このように、第1の契約者側に設けられた情報サーバは、情報を利用できる端末を制限するための実行権データを作成する。一方、第2の契約者側に設けられた他の情報サーバは、伝達された情報に付加された課金基準データを参照して、当該情報の利用料金を算定して記録する。1以上の端末はそれぞれ、伝達された実行権データが所定の条件を満たす場合に、伝達された情報の利用を許可する。これにより、第1の契約者が受信した情報を第2の契約者が利用する場合、利用度合に応じて、第2の契約者に課金できる。

【0139】第59の発明は、第58の発明において、1以上の情報提供者が提供する情報は、それぞれ暗号化されており、受信手段が受信した情報を復号する復号手段をさらに備えることを特徴としている。

【0140】これにより、1以上の情報提供者が提供する情報が暗号化されている場合、当該情報を復号できる。

【0141】第60の発明は、第59の発明において、1以上の端末はそれぞれ、情報サーバから伝達された、再暗号化された情報を、情報サーバから伝達された実行権データが所定の条件を満たす場合に復号する機能を有しており、復号手段が復号して得られた情報を、所定の方式で再暗号化する共通暗号化手段をさらに備えることを特徴としている。

【0142】これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0143】第61の発明は、第59の発明において、1以上の端末はそれぞれ、情報サーバから伝達された、再暗号化された情報を、情報サーバから伝達された実行権データが所定の条件を満たす場合に、情報サーバから伝達された乱数で復号する機能を有しており、乱数を発生する乱数発生手段と、復号手段が復号して得られた情報を、乱数発生手段が発生する乱数で再暗号化する共通暗号化手段とをさらに備えることを特徴としている。

【0144】上記のように、第61の発明では、乱数発生手段が乱数を発生し、共通暗号化手段は、復号手段が復号して得られた情報を、当該乱数で再暗号化する。再暗号化された情報、発生された乱数および作成された実行権データが第2の契約者側に伝達されると、1以上の端末はそれぞれ、伝達された、再暗号化された情報を、伝達された実行権データが所定の条件を満たす場合に、伝達された乱数で復号する。これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0145】第62の発明は、第61の発明において、共通暗号化手段が再暗号化して得られた情報は、書き込み/読み出し可能な携帯型記録媒体を介して、乱数発生手段が発生した乱数および実行権データ作成手段が作成した実行権データは、記録内容の解析/変更が困難な携帯型記録媒体を介して、それぞれ第2の契約者側に伝達されることを特徴としている。

【0146】これにより、第1の契約者側から第2の契約者側に、安全に情報を伝達できる。

【0147】第63の発明は、第59の発明において、1以上の端末はそれぞれ、情報サーバから伝達された、暗号化された乱数および実行権データを復号し、かつ、情報サーバから伝達された、再暗号化された情報を、復号して得た実行権データが所定の条件を満たす場合に、復号して得た乱数で復号する機能を有しており、乱数を発生する乱数発生手段と、復号手段が復号して得られた情報を、乱数発生手段が発生する乱数で再暗号化し、かつ、乱数発生手段が発生した乱数および実行権データ作成手段が作成した実行権データを所定の方式で暗号化する共通暗号化手段とをさらに備えることを特徴としている。

【0148】上記のように、第63の発明では、乱数発生手段が乱数を発生し、共通暗号化手段は、復号手段が復号して得られた情報を当該乱数で再暗号化し、かつ当該乱数および実行権データ作成手段が作成した実行権データを所定の方式で暗号化する。再暗号化された情報ならびに暗号化された乱数および実行権データが第2の契約者側に伝達されると、1以上の端末はそれぞれ、伝達された、暗号化された乱数および実行権データを復号し、さらに、伝達された、再暗号化された情報を、復号して得た実行権データが所定の条件を満たす場合に、復号して得た乱数で復号する。これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0149】第64の発明は、第63の発明において、共通暗号化手段が再暗号化して得られた情報ならびに共通暗号化手段が暗号化して得られた乱数および実行権データは、伝送速度が比較的大きい伝送路を介して、第2の契約者側に伝達されることを特徴としている。

【0150】第65の発明は、第63の発明において、

共通暗号化手段が再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、共通暗号化手段が暗号化して得られた乱数および実行権データは、伝送速度が比較的小さい伝送路を介して、それぞれ第2の契約者側に伝達されることを特徴としている。

【0151】第64および第65の発明により、第1の契約者側から第2の契約者側に、安全に情報を伝達できる。

【0152】第66の発明は、1以上の情報提供者と第1および第2の契約者とからなり、情報提供者は、第1の契約者に情報を提供し、第1の契約者は、提供される情報を第2の契約者に再提供して、第2の契約者が情報提供者に利用料金を支払うような情報提供システムの第2の契約者側に設けられる情報サーバであって、1以上の情報提供者はそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信し、第1の契約者側には、1以上の情報提供者が提供する情報を受信し、かつ受信した情報を利用可能な端末を制限するための実行権データを作成する機能を有する他の情報サーバが設けられており、第2の契約者側には、さらに、他の情報サーバから伝達された実行権データが所定の条件を満たす場合に、他の情報サーバから伝達された情報の利用を許可する機能を有する1以上の端末が設けられており、他の情報サーバから伝達された情報に付加された課金基準データに基づいて、当該情報の利用料金を算定する課金手段と、課金手段が算定して得られた利用料金を記録するデータ記録手段とを備えている。

【0153】上記のように、第66の発明では、1以上の情報提供者はそれぞれ、提供しようとする情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する。第1の契約者側に設けられた他の情報サーバは、1以上の情報提供者が提供する情報を受信して、当該情報を利用可能な端末を制限するための実行権データを作成する。受信された情報および作成された実行権データが第2の契約者側に伝達されると、情報サーバの課金手段は、伝達された情報に付加された課金基準データに基づいて、当該情報の利用料金を算定する。データ記録手段は、課金手段が算定して得られた利用料金を記録する。1以上の端末はそれぞれ、伝達された実行権データが所定の条件を満たす場合に、伝達された情報の利用を許可する。

【0154】このように、第1の契約者側に設けられた他の情報サーバは、情報を利用できる端末を制限するための実行権データを作成する。一方、第2の契約者側に設けられた情報サーバは、伝達された情報に付加された課金基準データを参照して、当該情報の利用料金を算定して記録する。1以上の端末はそれぞれ、伝達された実行権データが所定の条件を満たす場合に、伝達された情報の利用を許可する。これにより、第1の契約者が受信

した情報を第2の契約者が利用する場合、利用度合に応じて、第2の契約者に課金できる。

【0155】第67の発明は、第66の発明において、1以上の情報提供者が提供する情報は、それぞれ暗号化されており、他の情報サーバは、受信した情報を復号する機能をさらに有することを特徴としている。

【0156】これにより、1以上の情報提供者が提供する情報が暗号化されている場合、他の情報サーバは、当該情報を復号できる。

10 【0157】第68の発明は、第67の発明において、他の情報サーバは、復号して得た情報を所定の方式で再暗号化する機能をさらに有し、1以上の端末はそれぞれ、他の情報サーバから伝達された、再暗号化された情報を、他の情報サーバから伝達された実行権データが所定の条件を満たす場合に復号する機能を有することを特徴としている。

【0158】これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

20 【0159】第69の発明は、第67の発明において、他の情報サーバは、乱数を発生し、かつ復号して得た情報を当該乱数で再暗号化する機能をさらに有し、1以上の端末はそれぞれ、他の情報サーバから伝達された、再暗号化された情報を、他の情報サーバから伝達された実行権データが所定の条件を満たす場合に、他の情報サーバから伝達された乱数で復号する機能を有することを特徴としている。

30 【0160】上記のように、第69の発明では、他の情報サーバは、乱数を発生し、復号して得た情報を、当該乱数で再暗号化する。再暗号化された情報、発生された乱数および作成された実行権データが第2の契約者側に伝達されると、1以上の端末はそれぞれ、伝達された、再暗号化された情報を、伝達された実行権データが所定の条件を満たす場合に、伝達された乱数で復号する。これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

40 【0161】第70の発明は、第69の発明において、他の情報サーバが再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、他の情報サーバが発生した乱数および作成した実行権データは、記録内容の解析／変更が困難な携帯型記録媒体を介して、それぞれ第2の契約者側に伝達されることを特徴としている。

【0162】これにより、第1の契約者側から第2の契約者側に、安全に情報を伝達できる。

50 【0163】第71の発明は、第67の発明において、他の情報サーバは、乱数を発生し、かつ復号して得た情報を当該乱数で再暗号化し、かつ当該乱数および作成した実行権データを所定の方式で暗号化する機能をさらに有し、1以上の端末はそれぞれ、他の情報サーバから伝

達された、暗号化された乱数および実行権データを復号し、かつ、他の情報サーバから伝達された、再暗号化された情報を、復号して得た実行権データが所定の条件を満たす場合に、復号して得た乱数で復号する機能を有することを特徴としている。

【0164】上記のように、第71の発明では、他の情報サーバは、乱数を発生し、復号して得た情報を当該乱数で再暗号化し、さらに、当該乱数および作成した実行権データを所定の方式で暗号化する。再暗号化された情報ならびに暗号化された乱数および実行権データが第2の契約者側に伝達されると、1以上の端末はそれぞれ、伝達された、暗号化された乱数および実行権データを復号し、さらに、伝達された、再暗号化された情報を、復号して得た実行権データが所定の条件を満たす場合に、復号して得た乱数で復号する。これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0165】第72の発明は、第71の発明において、他の情報サーバが再暗号化して得られた情報ならびに他の情報サーバが暗号化して得られた乱数および実行権データは、伝送速度が比較的大きい伝送路を介して、第2の契約者側に伝達されることを特徴としている。

【0166】第73の発明は、第71の発明において、他の情報サーバが再暗号化して得られた情報は、書き込み/読み出し可能な携帯型記録媒体を介して、他の情報サーバが暗号化して得られた乱数および実行権データは、伝送速度が比較的小さい伝送路を介して、それぞれ第2の契約者側に伝達されることを特徴としている。

【0167】第72および第73の発明により、第1の契約者側から第2の契約者側に、安全に情報を伝達できる。

【0168】第74の発明は、1以上の情報提供者と第1および第2の契約者とからなり、情報提供者は、第1の契約者に情報を提供し、第1の契約者は、提供される情報を第2の契約者に再提供して、第2の契約者が情報提供者に利用料金を支払うような情報提供システムの第2の契約者側に設けられる端末であって、1以上の情報提供者はそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信し、第1の契約者側には、1以上の情報提供者が提供する情報を受信し、かつ受信した情報を利用可能な端末を制限するための実行権データを作成する機能を有する第1の情報サーバが設けられており、第2の契約者側には、さらに、第1の情報サーバから伝達された情報に付加された課金基準データに基づいて、当該情報の利用料金を算定し、かつ算定して得た利用料金を記録する機能を有する第2の情報サーバが設けられており、第1の情報サーバから伝達された実行権データが所定の条件を満たす場合に、第1の情報サーバから伝達された情報の利用を許可することを特徴としている。

【0169】上記のように、第74の発明では、1以上の情報提供者はそれぞれ、提供しようとする情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する。第1の契約者側に設けられた第1の情報サーバは、1以上の情報提供者が提供する情報を受信し、かつ、当該情報を利用可能な端末を制限するための実行権データを作成する。受信された情報および作成された実行権データが第2の契約者側に伝達されると、第2の情報サーバは、伝達された情報に付加された課金基準データに基づいて、当該情報の利用料金を算定し、かつ算定して得た利用料金を記録する。端末は、伝達された実行権データが所定の条件を満たす場合に、伝達された情報の利用を許可する。

【0170】このように、第1の契約者側の第1の情報サーバは、情報を利用できる端末を制限するための実行権データを作成する。一方、第2の契約者側の第2の情報サーバは、伝達された情報に付加された課金基準データを参照して、当該情報の利用料金を算定して記録する。端末は、伝達された実行権データが所定の条件を満たす場合に、伝達された情報の利用を許可する。これにより、第1の契約者が受信した情報を第2の契約者が利用する場合、利用度合に応じて、第2の契約者に課金できる。

【0171】第75の発明は、第74の発明において、1以上の情報提供者が提供する情報は、それぞれ暗号化されており、第1の情報サーバは、受信した情報を復号する機能をさらに有することを特徴としている。

【0172】これにより、1以上の情報提供者が提供する情報が暗号化されている場合、第1の情報サーバは、当該情報を復号できる。

【0173】第76の発明は、第75の発明において、第1の情報サーバは、復号して得た情報を所定の方式で再暗号化する機能をさらに有し、第1の情報サーバから伝達された、再暗号化された情報を、第1の情報サーバから伝達された実行権データが所定の条件を満たす場合に復号する復号手段を備えることを特徴としている。

【0174】これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0175】第77の発明は、第75の発明において、第1の情報サーバは、乱数を発生し、かつ復号して得た情報を当該乱数で再暗号化する機能をさらに有し、第1の情報サーバから伝達された、再暗号化された情報を、第1の情報サーバから伝達された実行権データが所定の条件を満たす場合に、第1の情報サーバから伝達された乱数で復号する復号手段を備えることを特徴としている。

【0176】上記のように、第77の発明では、第1の情報サーバは、乱数を発生し、復号して得た情報を、当該乱数で再暗号化する。再暗号化された情報、発生され

た乱数および作成された実行権データが第2の契約者側に伝達されると、端末の復号手段は、伝達された、再暗号化された情報を、伝達された実行権データが所定の条件を満たす場合に、伝達された乱数で復号する。これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0177】第78の発明は、第77の発明において、第1の情報サーバが再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、第1の情報サーバが発生した乱数および作成した実行権データは、記録内容の解析／変更が困難な携帯型記録媒体を介して、それぞれ第2の契約者側に伝達されることを特徴としている。

【0178】これにより、第1の契約者側から第2の契約者側に、安全に情報を伝達できる。

【0179】第79の発明は、第75の発明において、第1の情報サーバは、乱数を発生し、かつ復号して得た情報を当該乱数で再暗号化し、かつ当該乱数および作成した実行権データを所定の方式で暗号化する機能をさらに有し、第1の情報サーバから伝達された、暗号化された乱数および実行権データを復号し、かつ第1の情報サーバから伝達された、再暗号化された情報を、復号して得た実行権データが所定の条件を満たす場合に、復号して得た乱数で復号する復号手段を備えることを特徴としている。

【0180】上記のように、第79の発明では、第1の情報サーバは、乱数を発生し、復号して得た情報を当該乱数で再暗号化し、さらに、当該乱数および作成した実行権データを所定の方式で暗号化する。再暗号化された情報ならびに暗号化された乱数および実行権データが第2の契約者側に伝達されると、端末の復号手段は、伝達された、暗号化された乱数および実行権データを復号し、さらに、伝達された、再暗号化された情報を、復号して得た実行権データが所定の条件を満たす場合に、復号して得た乱数で復号する。これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0181】第80の発明は、第79の発明において、第1の情報サーバが再暗号化して得られた情報ならびに第1の情報サーバが暗号化して得られた乱数および実行権データは、伝送速度が比較的大きい伝送路を介して、第2の契約者側に伝達されることを特徴としている。

【0182】第81の発明は、第79の発明において、第1の情報サーバが再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、第1の情報サーバが暗号化して得られた乱数および実行権データは、伝送速度が比較的小さい伝送路を介して、それぞれ第2の契約者側に伝達されることを特徴としている。

【0183】第80および第81の発明により、第1の契約者側から第2の契約者側に、安全に情報を伝達でき

る。

【0184】第82の発明は、1以上の情報提供者と契約者とは、情報提供者は、契約者に情報を提供し、契約者は、提供される情報を利用して、情報提供者に利用料金を支払うような情報提供方法であって、1以上の情報提供者はそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信し、契約者側には、情報サーバおよび当該情報サーバに情報伝達可能に接続された1以上の端末が設けられ、情報サーバは、1以上の情報提供者が提供する情報を受信し、受信した情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定し、算定して得た利用料金を記録することを特徴としている。

【0185】上記のように、第82の発明では、1以上の情報提供者は、提供しようとする情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する。契約者側には情報サーバおよび1以上の端末が設けられており、情報サーバは、受信した情報に付加された課金基準データに基づいて、当該情報の利用料金を算定し、算定して得た利用料金を記録する。なお、記録された利用料金は、所定の方法で情報提供者に通知され、契約者は当該料金を支払うことになる。このように、情報サーバは、提供される情報毎に、利用料金を算定し、算定して得た利用料金を記録するため、契約者の利用度合に応じた課金ができる。

【0186】第83の発明は、第82の発明において、1以上の情報提供者が提供する情報は、それぞれ暗号化されており、情報サーバは、さらに、受信した情報を復号することを特徴としている。

【0187】これにより、1以上の情報提供者が提供する情報が暗号化されている場合、情報サーバは、当該情報を復号できる。

【0188】第84の発明は、第83の発明において、情報サーバは、1以上の端末毎の秘密鍵を記憶しており、さらに、復号して得た情報を、当該秘密鍵でそれぞれ再暗号化し、1以上の端末はそれぞれ、自己の秘密鍵を記憶しており、情報サーバから伝達された、再暗号化された情報を、当該秘密鍵で復号することを特徴としている。

【0189】上記のように、第84の発明では、情報サーバは、復号して得た情報を、1以上の端末毎の秘密鍵で再暗号化する。再暗号化された情報が1以上の端末に伝達されると、1以上の端末はそれぞれ、再暗号化された情報を、自己の秘密鍵で復号する。これにより、情報サーバから1以上の端末に、安全に情報を伝達できる。

【0190】第85の発明は、第83の発明において、情報サーバは、1以上の端末毎の秘密鍵を記憶しており、さらに、乱数を発生し、復号して得た情報を、当該乱数で再暗号化し、当該乱数を、当該秘密鍵でそれぞれ暗号化し、1以上の端末はそれぞれ、自己の秘密鍵を記

憶しており、情報サーバから伝達された、暗号化された乱数を、当該秘密鍵で復号し、情報サーバから伝達された、再暗号化された情報を、復号して得た乱数で復号することを特徴としている。

【0191】上記のように、第85の発明では、情報サーバは、乱数を発生し、復号して得た情報を当該乱数で再暗号化し、さらに、当該乱数を1以上の端末毎の秘密鍵で暗号化する。再暗号化された情報および暗号化された乱数が1以上の端末に伝達されると、1以上の端末はそれぞれ、暗号化された乱数を自己の秘密鍵で復号し、さらに、再暗号化された情報を、復号して得た乱数で復号する。これにより、情報サーバから1以上の端末に、より安全に情報を伝達できる。

【0192】第86の発明は、第82の発明において、1以上の情報提供者はそれぞれ、提供すべき情報に、記録を許可するか否かを示す記録許可フラグをさらに付加して配信し、情報サーバは、受信した情報に付加されている記録許可フラグが、記録を許可するものである場合に、当該情報を記録し、記録した情報が、1以上の端末に伝達される毎に、当該情報の利用料金を算定することを特徴としている。

【0193】上記のように、第86の発明では、1以上の情報提供者は、提供しようとする情報に、記録を許可するか否かを示す記録許可フラグを、さらに付加して配信する。情報サーバは、受信した情報に付加された記録許可フラグが記録を許可するものである場合に、当該情報を記録することができる。そして、情報サーバは、記録した情報が1以上の端末に伝達される毎に、利用料金を算定する。これにより、情報が記録されるのを制限することができ、かつ、契約者が情報を記録して繰り返し利用する場合、利用度合に応じて課金できる。

【0194】第87の発明は、第86の発明において、1以上の情報提供者が提供する情報は、それぞれ暗号化されており、情報サーバは、さらに、記録した情報を復号することを特徴としている。

【0195】このように、1以上の情報提供者が提供する情報が暗号化されている場合、情報サーバは、受信した情報を暗号化されたままで記録し、当該情報が端末に伝達される際に復号することにより、記録された情報が不正に利用されるのを防ぐことができる。

【0196】第88の発明は、第87の発明において、情報サーバは、1以上の端末毎の秘密鍵を記憶しており、さらに、復号して得た情報を、当該秘密鍵でそれぞれ再暗号化し、1以上の端末はそれぞれ、自己の秘密鍵を記憶しており、情報サーバから伝達された、再暗号化された情報を、当該秘密鍵で復号することを特徴としている。

【0197】上記のように、第88の発明では、情報サーバは、復号して得た情報を、1以上の端末毎の秘密鍵で再暗号化する。再暗号化された情報が1以上の端末に

伝達されると、1以上の端末はそれぞれ、伝達された、再暗号化された情報を、自己の秘密鍵で復号する。これにより、情報サーバから1以上の端末に、安全に情報を伝達できる。

【0198】第89の発明は、第87の発明において、情報サーバは、1以上の端末毎の秘密鍵を記憶しており、さらに、乱数を発生し、復号して得た情報を、当該乱数で再暗号化し、当該乱数を、当該秘密鍵でそれぞれ暗号化し、1以上の端末はそれぞれ、自己の秘密鍵を記憶しており、情報サーバから伝達された、暗号化された乱数を、当該秘密鍵で復号し、情報サーバから伝達された、再暗号化された情報を、復号して得た乱数で復号することを特徴としている。

【0199】上記のように、第89の発明では、情報サーバは、乱数を発生し、復号して得た情報を当該乱数で再暗号化し、さらに、当該乱数を1以上の端末毎の秘密鍵で暗号化する。再暗号化された情報および暗号化された乱数が1以上の端末に伝達されると、1以上の端末はそれぞれ、伝達された、暗号化された乱数を、自己の秘密鍵で復号し、さらに、伝達された、再暗号化された情報を、復号して得た乱数で復号する。これにより、情報サーバから1以上の端末に、より安全に情報を伝達できる。

【0200】第90の発明は、1以上の情報提供者と契約者とからなり、情報提供者は、契約者に情報を提供し、契約者は、提供される情報を利用して、情報提供者に利用料金を支払うような情報提供方法であって、1以上の情報提供者はそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信し、契約者側には、情報サーバおよびオフライン端末が設けられ、情報サーバは、1以上の情報提供者が提供する情報を受信し、受信した情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成し、作成した実行権データおよび受信した情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定し、算定して得た利用料金を記録し、オフライン端末は、情報サーバから伝達された実行権データが所定の条件を満たす場合に、情報サーバから伝達された情報の利用を許可することを特徴としている。

【0201】上記のように、第90の発明では、1以上の情報提供者は、提供しようとする情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する。契約者側には情報サーバおよびオフライン端末が設けられており、情報サーバは、提供される情報を受信すると、当該情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成する。次に、情報サーバは、作成した実行権データ、および受信した情報に付加された課金基準データに基づいて、当該情報の利用料金を算定して記録する。なお、記録された利用料金は所定の方法で情報提供者に通知され、契約者

は当該料金を支払うことになる。受信された情報および作成された実行権データがオフライン端末に伝達されると、オフライン端末は、伝達された実行権データが所定の条件を満たす場合に、伝達された情報を利用するのを許可する。

【0202】このように、情報サーバは、情報の利用度合および情報を利用できる端末を制限するための実行権データを作成し、同時に、当該情報に付加された課金基準データを参照して、作成した実行権データに応じた利用料金を算定して記録する。オフライン端末は、伝達された実行権データが所定の条件を満たす場合に、伝達された情報を利用するのを許可する。これにより、契約者がオフライン端末において情報を利用する場合、利用度合に応じて課金できる。

【0203】第91の発明は、第90の発明において、1以上の情報提供者が提供する情報は、それぞれ暗号化されており、情報サーバは、さらに、受信した情報を復号することを特徴としている。

【0204】これにより、1以上の情報提供者が提供する情報が暗号化されている場合、情報サーバは、当該情報を復号できる。

【0205】第92の発明は、第91の発明において、情報サーバは、さらに、復号して得た情報を所定の方法で再暗号化し、オフライン端末は、情報サーバから伝達された、再暗号化された情報を、情報サーバから伝達された実行権データが所定の条件を満たす場合に復号することを特徴としている。

【0206】これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0207】第93の発明は、第91の発明において、情報サーバは、さらに、乱数を発生し、復号して得た情報を、当該乱数で再暗号化し、オフライン端末は、情報サーバから伝達された、再暗号化された情報を、情報サーバから伝達された実行権データが所定の条件を満たす場合に、情報サーバから伝達された乱数で復号することを特徴としている。

【0208】上記のように、第93の発明では、情報サーバは、乱数を発生し、復号して得た情報を、当該乱数で再暗号化する。再暗号化された情報、発生された乱数および作成された実行権データがオフライン端末に伝達されると、オフライン端末は、伝達された、再暗号化された情報を、伝達された実行権データが所定の条件を満たす場合に、伝達された乱数で復号する。これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

【0209】第94の発明は、第93の発明において、情報サーバが再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、情報サーバが発生した乱数および作成した実行権データは、記録内容

の解析／変更が困難な携帯型記録媒体を介して、それぞれオフライン端末に伝達されることを特徴としている。

【0210】これにより、情報サーバからオフライン端末に、安全に情報を伝達できる。

【0211】第95の発明は、1以上の情報提供者と第1および第2の契約者とからなり、情報提供者は、第1の契約者に情報を提供し、第1の契約者は、提供される情報を第2の契約者に再提供して、第1または第2の契約者のいずれかが、情報提供者に利用料金を支払うような情報提供方法であって、1以上の情報提供者はそれぞれ、提供すべき情報に、当該情報の利用料金を算定するための課金基準データを付加して配信し、第1の契約者側には第1の情報サーバが、第2の契約者側には、第2の情報サーバおよび当該サーバに情報伝達可能に接続された1以上の端末が、それぞれ設けられ、第1の契約者に課金する場合、第1の情報サーバは、1以上の情報提供者が提供する情報を受信し、受信した情報の利用度合および当該情報を利用可能な端末を制限するための実行権データを作成し、作成した実行権データおよび受信した情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定し、算定して得た利用料金を記録し、1以上の端末はそれぞれ、第1の情報サーバから伝達された実行権データが所定の条件を満たす場合に、第1の情報サーバから伝達された情報の利用を許可し、第2の契約者に課金する場合には、第1の情報サーバは、1以上の情報提供者が提供する情報を受信し、受信した情報を利用可能な端末を制限するための実行権データを作成し、第2の情報サーバは、第1の情報サーバから伝達された情報に付加されている課金基準データに基づいて、当該情報の利用料金を算定し、算定して得た利用料金を記録し、1以上の端末はそれぞれ、第1の情報サーバから伝達された実行権データが所定の条件を満たす場合に、第1の情報サーバから伝達された情報の利用を許可することを特徴としている。

【0212】上記のように、第95の発明では、1以上の情報提供者は、提供しようとする情報に、当該情報の利用料金を算定するための課金基準データを付加して配信する。第1の契約者側には第1の情報サーバが、第2の契約者側には第2の情報サーバおよび1以上の端末が、それぞれ設けられており、第1の情報サーバは、提供される情報を受信する。第1の契約者に課金する場合、第1の情報サーバは、受信した情報の利用度合、および当該情報を利用できる端末を制限するための実行権データを作成し、かつ、作成した実行権データ、および当該情報に付加された課金基準データに基づいて、当該情報の利用料金を算定して記録する。なお、記録された利用料金は、所定の方法で各情報提供者に通知され、第1の契約者が当該料金を支払うことになる。受信された情報および作成された実行権データが第2の契約者に伝達されると、1以上の端末はそれぞれ、伝達された実行

権データが所定の条件を満たす場合に、伝達された情報の利用を許可する。

【0213】第2の契約者に課金する場合には、第1の情報サーバは、受信した情報を利用可能な端末を制限するための実行権データを作成する。受信された情報および作成された実行権データが第2の契約者に伝達されると、第2の情報サーバは、伝達された情報に付加された課金基準データに基づいて、当該情報の利用料金を算定して記録する。なお、記録された利用料金は、所定の方法で各情報提供者に通知され、第2の契約者が当該料金を支払うことになる。一方、1以上の端末はそれぞれ、伝達された実行権データが所定の条件を満たす場合に、伝達された情報を利用するのを許可する。

【0214】このように、第1の契約者が受信した情報を第2の契約者が利用して、第1の契約者に課金する場合、第1の契約者側の第1の情報サーバは、情報の利用度合および情報を利用できる端末を制限するための実行権データを作成し、同時に、当該情報に付加された課金基準データを参照して、作成した実行権データに応じた利用料金を算定し、算定して得た利用料金を記録する。1以上の端末はそれぞれ、伝達された実行権データが所定の条件を満たす場合に、伝達された情報を利用するのを許可する。これにより、第2の契約者の利用度合に応じて、第1の契約者に課金することができる。なお、第1の契約者が受信した情報を第2の契約者が利用して、第1の契約者に課金するという提供形態は、情報をプレゼントするという、情報提供の新たな形態である。

【0215】第2の契約者に課金する場合には、第1の情報サーバは、情報を利用できる端末を制限するための実行権データを作成し、一方、第2の情報サーバは、当該情報に付加された課金基準データを参照して、当該情報の利用料金を算定し、算定して得た利用料金を記録する。1以上の端末はそれぞれ、伝達された実行権データが所定の条件を満たす場合、伝達された情報を利用するのを許可する。これにより、第2の契約者の利用度合に応じて、第2の契約者に課金することができる。

【0216】第96の発明は、第95の発明において、1以上の情報提供者が提供する情報は、それぞれ暗号化されており、第1の情報サーバは、さらに、受信した情報を復号することを特徴としている。

【0217】これにより、1以上の情報提供者が提供する情報が暗号化されている場合、第1の情報サーバは、当該情報を復号できる。

【0218】第97の発明は、第96の発明において、第1の情報サーバは、さらに、復号して得た情報を所定的方式で再暗号化し、1以上の端末はそれぞれ、第1の情報サーバから伝達された、再暗号化された情報を、第1の情報サーバから伝達された実行権データが所定の条件を満たす場合に復号することを特徴としている。

【0219】これにより、実行権データが所定の条件を

満たす場合にのみ、情報を利用可能にすることができる。

【0220】第98の発明は、第96の発明において、第1の情報サーバは、さらに、乱数を発生し、復号して得た情報を、当該乱数で再暗号化し、1以上の端末はそれぞれ、第1の情報サーバから伝達された、再暗号化された情報を、第1の情報サーバから伝達された実行権データが所定の条件を満たす場合に、第1の情報サーバから伝達された乱数で復号することを特徴としている。

10 【0221】上記のように、第98の発明では、第1の情報サーバは、乱数を発生し、復号して得た情報を当該乱数で再暗号化する。再暗号化された情報、作成された実行権データおよび発生された乱数が第2の契約者側に伝達されると、1以上の端末はそれぞれ、伝達された、再暗号化された情報を、伝達された実行権データが所定の条件を満たす場合に、伝達された乱数で復号する。これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

20 【0222】第99の発明は、第98の発明において、第1の情報サーバが再暗号化して得られた情報は、書き込み/読み出し可能な携帯型記録媒体を介して、第1の情報サーバが発生した乱数および作成した実行権データは、記録内容の解析/変更が困難な携帯型記録媒体を介して、それぞれ第2の契約者側に伝達されることを特徴としている。

【0223】これにより、第1の契約者側から第2の契約者側に、安全に情報を伝達できる。

30 【0224】第100の発明は、第96の発明において、第1の情報サーバは、さらに、乱数を発生し、復号して得た情報を、当該乱数で再暗号化し、当該乱数および作成した実行権データを、所定的方式で暗号化し、1以上の端末はそれぞれ、第1の情報サーバから伝達された、暗号化された乱数および実行権データを復号し、第1の情報サーバから伝達された、再暗号化された情報を、復号して得た実行権データが所定の条件を満たす場合に、復号して得た乱数で復号することを特徴としている。

40 【0225】上記のように、第100の発明では、第1の情報サーバは、乱数を発生し、復号して得た情報を当該乱数で再暗号化し、さらに、当該乱数および作成した実行権データを所定的方式で暗号化する。再暗号化された情報ならびに暗号化された乱数および実行権データが第2の契約者側に伝達されると、1以上の端末はそれぞれ、伝達された、暗号化された実行権データおよび乱数を復号し、さらに、伝達された、再暗号化された情報を、復号して得た実行権データが所定の条件を満たす場合に、復号して得た乱数で復号する。これにより、実行権データが所定の条件を満たす場合にのみ、情報を利用可能にすることができる。

50 【0226】第101の発明は、第100の発明におい

て、第1の情報サーバが再暗号化して得られた情報ならびに第1の情報サーバが暗号化して得られた乱数および実行権データは、伝送速度が比較的大きい伝送路を介して、第2の契約者側に伝達されることを特徴としている。

【0227】第102の発明は、第100の発明において、第1の情報サーバが再暗号化して得られた情報は、書き込み／読み出し可能な携帯型記録媒体を介して、第1の情報サーバが暗号化して得られた乱数および実行権データは、伝送速度が比較的小さい伝送路を介して、それぞれ第2の契約者側に伝達されることを特徴としている。

【0228】第101および第102の発明により、第1の契約者側から第2の契約者側に、安全に情報を伝達できる。

【0229】

【発明の実施の形態】図1は、本発明の一実施形態に係る情報提供システムの構成を示すブロック図である。図1のシステムは、情報提供者X1、情報提供者Y2および情報提供者Z3ならびに契約者A4および契約者B5で構成されている。なお、契約者とは、1以上のユーザからなる、一つの世帯を意味する。契約者A4と契約者B5とは、通信回線／CATV網を介して、または、携帯型の記録媒体を介して、双方向に情報のやりとりを行うことができる。ただし、以下では、携帯型の記録媒体を介して情報のやりとりを行う場合に限定して説明する。

【0230】情報提供者X1、情報提供者Y2および情報提供者Z3はそれぞれ、契約者A4および契約者B5に、衛星放送、地上波放送、デジタルCATV網などを介して、映像情報、文字情報などの情報を提供する。その際、各情報提供者（1～3）は、それぞれが定めた配信方式、暗号方式および課金方式を用いることができる。

【0231】契約者A4および契約者B5はそれぞれ、各情報提供者（1～3）が提供する情報を利用して、各情報提供者（1～3）に、定期的に利用料金を支払う。ただし、利用料金は、契約者（4、5）毎に、情報を利用した度合に応じて算定される。なお、算定された利用料金は、電話回線、パソコン通信網、デジタルCATV網などを通じて、各情報提供者（1～3）に通知される。

【0232】各情報提供者（1～3）は、提供しようとする情報を暗号化したうえ、情報識別子、課金基準データおよび記録許可フラグを付加して提供する。ここで、情報識別子は、その情報を他の情報と区別するためのものであって、どの情報提供者（1～3）から提供された情報であるかを示すデータも含まれる。課金基準データは、その情報の利用料金を算定するためのデータであって、リアルタイムに利用する場合の利用料金、記録して

利用する場合の利用料金などのデータを含んでいる。記録許可フラグは、その情報を契約者（4、5）側で記録できるか否かを示すフラグであって、その情報が、記録できるものであれば1、記録できないものであれば0と定められている。

【0233】図1の契約者A4は、情報サーバ10a、1以上のユーザ端末20a、移動ディスク30a、ICカード40aおよびオフライン端末50aを備えている。移動ディスク30aは、書き込み／読み出しが可能な携帯型の記録媒体であり、ICカード40aは、記録されたデータの不正な解析／変更が困難な携帯型の記録媒体である。情報サーバ10aは、受信した情報をユーザ端末20aに送信し、かつ、移動ディスク30aおよびICカード40aに、それぞれ、情報、データ類を記録する。ユーザ端末20aは、情報サーバ10aから送信された情報を受信し、かつ、移動ディスク30aおよびICカード40aにそれぞれ記録された、情報、データ類を読み出す。ユーザ端末20aはまた、ユーザが入力する命令等を情報サーバ10aに伝達することができる。オフライン端末50aは、移動ディスク30aおよびICカード40aにそれぞれ記録された、情報、データ類を読み出す。

【0234】図1の情報サーバ10aは、Xの受信部101a、Xの復号部102a、Xの課金部103a、Yの受信部104a、Yの復号部105a、Yの課金部106a、Zの受信部107a、Zの復号部108a、Zの課金部109a、情報記録部110a、共通暗号化部111a、データ記録部112aおよび乱数発生部113aを備えている。

【0235】Xの受信部101aは、情報提供者X1が配信する情報を受信する。Xの復号部102aは、Xの受信部101aが受信した情報、および情報記録部110aに記録された情報のうち情報提供者X1が提供した情報を復号する。Xの課金部103aは、Xの復号部102aが復号する情報に付加されている課金基準データに基づいて、その情報の利用料金を算定する。Xの課金部103aはまた、必要に応じて、実行権データを作成する。Yの受信部104aは、情報提供者Y2が配信する情報を受信する。Yの復号部105aは、Yの受信部104aが受信した情報、および情報記録部110aに記録された情報のうち情報提供者Y2が提供した情報を復号する。Yの課金部106aは、Yの復号部105aが復号する情報に付加されている課金基準データに基づいて、その情報の利用料金を算定する。Yの課金部106aはまた、必要に応じて、実行権データを作成する。Zの受信部107aは、情報提供者Z3が配信する情報を受信する。Zの復号部108aは、Zの受信部107aが受信した情報、および情報記録部110aに記録された情報のうち情報提供者Z3が提供した情報を復号する。Zの課金部109aは、Zの復号部108aが復号

する情報に付加されている課金基準データに基づいて、その情報の利用料金を算定する。Zの課金部109aはまた、必要に応じて、実行権データを作成する。

【0236】ここで、実行権データとは、オフライン端末50aで情報を利用する場合や、契約者A4が受信した情報を契約者B5に再提供して、契約者B5のユーザがユーザ端末20bで情報を利用する場合に、その情報の利用度合およびその情報を利用可能な端末を制限するためのものであって、利用可能回数、記録モードおよび課金モードを含む。

【0237】利用可能回数は、その情報を利用することができる回数であり、利用にともなう更新される。記録モードは、その情報を利用可能な端末を限定するためのものであって、オフライン端末50aで利用する場合は1、契約者B5のユーザ端末20bで利用する場合には2と定められている。課金モードは、その情報が課金済みの情報であるか否かを示すものであって、課金済みであれば1、未課金であれば2と定められている。

【0238】情報記録部110aは、各受信部(101a、104a、107a)が受信した情報を記録する。ただし、情報記録部110aは、記録しようとする情報に付加された記録許可フラグが1であるか否かを判定する機能を有し、記録許可フラグが1でない情報は記録しない。データ記録部112aは、各課金部(103a、106a、109a)が算定して得られた利用料金を記録する。データ記録部112aはまた、ユーザ端末20a毎の秘密鍵を記憶している。乱数発生部113aは、乱数を発生する。

【0239】共通暗号化部111aは、本システムに共通の暗号化アルゴリズムを保有しており、当該アルゴリズムに従って、各復号部(102a、105a、108a)が復号して得られた情報を、乱数発生部113aが発生した乱数で再暗号化する。共通暗号化部111aはまた、秘密鍵暗号化アルゴリズムを保有しており、再暗号化して得た情報がユーザ端末20aに伝達される場合、乱数発生部113aが発生した乱数を、当該アルゴリズムに従って、データ記録部112aが記憶している、ユーザ端末20a毎の秘密鍵で暗号化する。なお、各課金部(103a、106a、109a)およびデータ記録部112aは、解析、変造ないしは複製ができないような領域に配置されている。

【0240】ユーザ端末20aは、共通復号部201aを備えている。共通復号部201aは、ユーザ端末20aに固有の秘密鍵、および秘密鍵復号アルゴリズムを保有しており、情報サーバ10aから伝達される、暗号化された乱数を、当該アルゴリズムに従って、この秘密鍵で復号する。共通復号部201aはまた、本システムに共通の復号アルゴリズムを保有しており、当該アルゴリズムに従って、情報サーバ10aから伝達される、再暗号化された情報を、復号して得た乱数で復号し、かつ、

情報サーバ10bから伝達される、再暗号化された情報を、情報サーバ10bから伝達される乱数で復号する。ただし、共通復号部201aは、情報サーバ10bから伝達される実行権データが所定の条件を満足するか否かを判定する機能を有しており、満足しない場合には、情報サーバ10bから伝達される、再暗号化された情報を、情報サーバ10bから伝達される乱数で復号する動作を行わない。

【0241】オフライン端末50aは、共通復号部501aを備えている。共通復号部501aは、本システムに共通の復号アルゴリズムを保有しており、情報サーバ10aから伝達される、再暗号化された情報を、当該アルゴリズムに従って、情報サーバ10aから伝達される乱数で復号する。ただし、共通復号部501aは、情報サーバ10aから伝達される実行権データが所定の条件を満足するか否かを判定する機能を有しており、満足しない場合には、再暗号化された情報を乱数で復号する動作を行わない。

【0242】なお、契約者B5についても、オフライン端末50aを含まない点を除いて、上記と同様である。ただし、図1において、契約者B5の各構成要素の参照番号は、情報サーバ10b、Xの復号部102bなどのように、契約者A4のものと区別されている。

【0243】以下には、情報提供者X1が提供する情報を、契約者A4が受信して、リアルタイムに利用する場合、記録して利用する場合、オフライン端末50aで利用する場合、および契約者A4が受信して、契約者B5が利用する場合について、それぞれ本システムの動作を説明する。

30 (1) リアルタイムに利用する場合

図2は、情報提供者X1が提供する情報を、契約者A4が受信して、リアルタイムに利用する場合の、図1のシステムの動作を示すフローチャートである。以下には、図2を用いて、図1の契約者A4が情報提供者X1から提供される情報を受信し、契約者A4のユーザが、その情報をユーザ端末20aでリアルタイムに利用する場合について説明する。ユーザが、情報提供者X1が提供している、ある情報を利用したい意を、ユーザ端末20aに入力すると、ユーザ端末20aは、その意を情報サーバ10aに通知する。

【0244】通知を受けると、情報サーバ10aのXの復号部102aは、Xの受信部101aが受信した、暗号化された情報を復号する(ステップS101)。Xの課金部103aは、その情報に付加されている課金基準データに基づいて、その情報の利用料金を算定する(ステップS102)。ただし、利用料金は、リアルタイムに情報を利用する場合の基準に基づいて算定される。Xの課金部103aが算定して得られた利用料金は、データ記録部112aが、情報提供者(1~3)毎に記録する(ステップS103)。なお、データ記録部112a

が記録した利用料金は、電話回線、パソコン通信網、ディジタルCATV網などを通じて、定期的に各情報提供者(1~3)に通知され、契約者A4は、その料金を支払うことになる。

【0245】次に、乱数発生部113aが乱数rを発生し、共通暗号化部111aは、Xの復号部102aが復号して得られた情報(CONT)を、本システムに共通の暗号化アルゴリズム(COM)に従って、乱数rで再暗号化する(ステップS104)。共通暗号化部111aは、さらに、秘密鍵暗号化アルゴリズム(E)に従って、データ記録部112aが記憶している、ユーザ端末20a毎の秘密鍵siで、乱数rを暗号化する(ステップS105)。情報サーバ10aは、共通暗号化部111aが再暗号化して得られた情報COM(r, CONT)および暗号化して得られた乱数E(si, r)を、ユーザ端末20aに送信する(ステップS106)。ここで、a(b, c)は、アルゴリズムaに従って、鍵bでデータcを暗号化することを意味する。

【0246】ユーザ端末20aが、再暗号化された情報COM(r, CONT)および暗号化された乱数E(si, r)を受信すると(ステップS107)、ユーザ端末20aの共通復号部201aは、最初、秘密鍵復号アルゴリズムに従って、記憶している秘密鍵siで、暗号化された乱数E(si, r)を復号して、乱数rを取り出し(ステップS108)、次に、再暗号化された情報COM(r, CONT)を、本システムに共通の復号アルゴリズムに従って、取り出した乱数rで復号して、情報(CONT)をさらに取り出す(ステップS109)。ユーザ端末20aは、共通復号部201aが復号して得られた情報(CONT)を表示する。こうして、ユーザは、情報(CONT)を利用することができる(ステップS110)。

【0247】このように、情報提供者X1は、提供しようとする情報を暗号化したうえ、その情報の利用料金を算定するための課金基準データを付加して提供する。契約者A4には、情報サーバ10aおよび1以上のユーザ端末20aが設けられ、情報サーバ10aのXの受信部101aは、情報提供者X1が提供する情報を受信する。Xの課金部103aは、Xの復号部102aが復号して得られた情報が、ユーザ端末20aに伝達される際に、その情報に付加された課金基準データに基づいて、その情報の利用料金を算定する。データ記録部112aは、Xの課金部103aが算定して得られた利用料金を記録する。なお、記録された利用料金は、所定の方法で情報提供者X1に通知され、契約者A4は、その料金を支払うことになる。これにより、契約者A4が情報をリアルタイムに利用する場合、利用度合に応じた課金ができる。

【0248】また、乱数発生部113aが乱数を発生し、共通暗号化部111aは、Xの復号部101aが復

号して得られた情報を、その乱数で再暗号化し、さらに、その乱数を、データ記録部112aが記憶しているユーザ端末20a毎の秘密鍵で暗号化する。再暗号化された情報および暗号化された乱数がユーザ端末20aに伝達されると、共通復号部201aは、伝達された、暗号化された乱数を自己の秘密鍵で復号し、さらに、復号して得た乱数で、伝達された、再暗号化された情報を復号する。これにより、情報サーバ10aからユーザ端末20aに、安全に情報を伝達できる。

10 【0249】なお、共通暗号化部111aは、Xの復号部101aが復号して得られた情報を、データ記録部112aが記憶しているユーザ端末20a毎の秘密鍵で再暗号化し、共通復号部201aは、伝達された、再暗号化された情報を、自己の秘密鍵で復号するようにしてもよい。ただし、この場合、情報は、毎回、同一の鍵で暗号化されるため、乱数で暗号化する場合に比べると、伝達時の安全性は低くなる。

【0250】(2)記録して利用する場合

図3は、情報提供者X1が提供する情報を、契約者A4が受信して記録し、記録した情報を利用する場合の、図1のシステムの動作を示すフローチャートである。以下には、図3を用いて、図1の契約者A4が情報提供者X1から提供される情報を受信して記録し、記録した情報を、契約者A4のユーザが利用する場合について説明する。ユーザが、情報提供者X1が提供している、ある情報を記録したい意を、ユーザ端末20aに入力すると、ユーザ端末20aは、その意を情報サーバ10aに通知する。

30 【0251】通知を受けると、情報サーバ10aの情報記録部110aは、Xの受信部101aが受信した情報に付加されている記録許可フラグが1であるか否か、すなわち、その情報が記録を許可されたものであるか否かを判定する(ステップS201)。付加された記録許可フラグが1である場合、すなわち、記録を許可された情報である場合、情報記録部110aは、その情報を記録する(ステップS202)。付加された記録許可フラグが1でない場合、すなわち、記録を許可されない情報である場合には、情報記録部110aは、その情報を記録せず、ユーザ端末20aが、エラーを表示する(ステップS203)。

40 【0252】ユーザが、上記のようにして情報記録部110aに記録された、ある情報を利用したい意を、ユーザ端末20aに入力すると(ステップS204)、情報サーバ10aは、付加された情報識別子を参照して、情報記録部110aに記録された情報のうち、ユーザが求める情報を見出す。そして、情報サーバ10aは、その情報が情報提供者X1から提供されたものであることを認識し、その情報をXの復号部102aに入力する。Xの復号部102aは、入力された情報を復号する(ステップS205)。

【0253】次に、Xの課金部103aは、その情報に付加された課金基準データに基づいて、その情報の利用料金を算定する（ステップS206）。ただし、利用料金は、情報を記録して利用する場合の基準に基づいて算定される。そして、データ記録部112aは、Xの課金部103aが算定して得られた利用料金を記録する（ステップS207）。以降、上記リアルタイムに利用する場合と同様にして、情報サーバ10aがその情報を再暗号化してユーザ端末20aに送信し、ユーザ端末20aは、情報サーバ10aから送信された、再暗号化された情報を受信して復号する（ステップS208～ステップS213）。こうして、ユーザは、情報記録部110aに記録された情報を利用することができる（ステップS214）。

【0254】このように、情報提供者X1は、提供しようとする情報に、さらに、記録許可フラグを付加して提供する。情報記録部110aは、Xの受信部101aが受信した情報に付加されている記録許可フラグが、記録を許可することを示す1である場合に、その情報を記録することができる。Xの課金部103aは、情報記録部110aが記録した情報が、ユーザ端末20aに送信される毎に、その情報に付加された課金基準データに基づいて、その情報の利用料金を算定する。これにより、契約者A4が情報を記録するのを制限することができ、かつ、契約者A4が情報を記録して繰り返し利用する場合、利用度合に応じた課金ができる。

【0255】また、情報記録部110aは、Xの受信部101aが受信した情報を、暗号化されたままで記録し、記録された情報がユーザ端末20aに伝達される際に、Xの復号部102aが、その情報を復号する。これにより、契約者A4が記録した情報が不正に利用されるのを防ぐことができる。

【0256】（3）オフライン端末50aで利用する場合

図4は、情報提供者X1が提供する情報を、契約者A4が受信して、オフライン端末50aで利用する場合の、図1のシステムの動作を示すフローチャートである。以下には、図4を用いて、図1の契約者A4が情報提供者X1から提供される情報を受信し、契約者A4のユーザが、その情報をオフライン端末50aで利用する場合について説明する。なお、情報提供者X1から提供された情報は、図3のステップS201～ステップS203と同様にして、情報記録部110aに記録されているものとする。

【0257】ユーザが、ユーザ端末20aに、情報記録部110aに記録された、ある情報を、オフライン端末50aで利用したい意を入力すると、ユーザ端末20aは、その意を情報サーバ10aに通知する。通知を受けると、情報サーバ10aは、付加された情報識別子を参照して、情報記録部110aに記録された情報のうち、

ユーザが求める情報を見出す。そして、情報サーバ10aは、その情報が情報提供者X1から提供されたものであることを認識し、その情報をXの復号部102aに入力する。Xの復号部102aは、入力された情報を復号する（ステップS301）。

【0258】次に、Xの課金部103aは、実行権データを作成する。実行権データには、利用可能回数、記録モードおよび課金モードが含まれ、この場合、利用可能回数は、ユーザが申告した、その情報を利用する回数であり、記録モードは、オフライン端末50aで利用されるべき情報であることを示す1、課金モードは、契約者A4に対して課金済みであることを示す1である。同時に、Xの課金部103aは、Xの復号部102aが復号して得られた情報に付加されている課金基準データに基づいて、作成した実行権に応じた利用料金、すなわち、その情報を、オフライン端末50aで、利用可能回数に等しい回数だけ利用する場合の利用料金を算定する（ステップS302）。そして、データ記録部112aは、Xの課金部103aが算定して得られた利用料金を記録する（ステップS303）。

【0259】Xの復号部102aが復号して得られた情報は、上記リアルタイムに利用する場合と同様にして再暗号化されたうえで、移動ディスク30aに記録される（ステップS304、ステップS305）。乱数発生部113aが発生した乱数rは、Xの課金部102aが作成した実行権データとともに、ICカード40aに記録される（ステップS306）。

【0260】次に、ユーザは、暗号化された情報が記録された移動ディスク30aと、乱数rおよび実行権データが記録されたICカード40aとを、オフライン端末50aに接続する（ステップS307）。オフライン端末50aの共通復号部501aは、最初、ICカード40aに記録された実行権データに含まれている記録モードが1であるか否かを判定する（ステップS308）。記録モードが1である場合、共通復号部501aは、実行権データに含まれる利用可能回数が1以上であるか否かを、さらに判定する（ステップS309）。

【0261】利用可能回数が1以上であれば、共通復号部501aは、ICカード40aに記録された乱数rで、移動ディスク30aに記録された情報を、上記リアルタイムに利用する場合と同様にして復号する（ステップS310）。そして、オフライン端末50aは、ICカード40aに記録されている利用可能回数を更新し（ステップS311）、次いで、共通復号部501aが復号して得られた情報を表示する。こうして、ユーザは、オフライン端末50aで、情報を利用することができる（ステップS312）。

【0262】ステップS308で、記録モードが1でない場合、もしくは、ステップS309で、利用可能回数が0である場合には、共通復号部501aは、暗号化さ

れた情報を乱数 r で復号する動作を行わず、オフライン端末 50a が、ユーザに対してエラーを通知する（ステップ S313）。

【0263】このように、Xの課金部103aは、情報の利用度合およびその情報を利用可能な端末を制限するための実行権データを作成し、同時に、その情報に付加された課金基準データをに基づいて、作成した実行権データに応じた利用料金を算定する。その情報およびXの課金部103aが作成した実行権データがオフライン端末50aに伝達されると、オフライン端末50aは、伝達された実行権データが所定の条件を満たす場合に、伝達された情報をユーザに表示する。これにより、契約者A4のユーザがオフライン端末50aで情報を利用する場合、利用度合に応じた課金ができる。

【0264】また、乱数発生部113aが乱数を発生し、共通暗号化部111aは、Xの復号部102aが復号して得られた情報を、その乱数で再暗号化する。再暗号化された情報、発生された乱数および作成された実行権データがオフライン端末50aに伝達されると、共通復号部501aは、伝達された、再暗号化された情報を、伝達された実行権データが所定の条件を満たす場合に、伝達された乱数で復号する。これにより、オフライン端末50aにおいて、実行権データが所定の条件を満たす場合にのみ、情報が表示されるようにすることができる。

【0265】なお、共通暗号化部111aは、Xの復号部101aが復号して得られた情報を、データ記録部112aが記憶しているユーザ端末20a毎の秘密鍵で再暗号化し、共通復号部201aは、伝達された、再暗号化された情報を、伝達された実行権データが所定の条件を満たす場合に、自己の秘密鍵で復号するようにしても、実行権データが所定の条件を満たす場合にのみ、情報が表示されるようにすることができる。

【0266】また、共通暗号化部111aが再暗号化して得られた情報は、移動ディスク30aのような、書き込み／読み出し可能な携帯型記録媒体を介して、乱数発生部113aが発生した乱数およびXの課金部103aが作成した実行権データは、ICカード40aのような、記録内容の解析／変更が困難な携帯型記録媒体を介して、それぞれオフライン端末50aに伝達することにより、情報サーバ10aからオフライン端末50aに、安全に情報を伝達できる。

【0267】（4）契約者A4が受信して、契約者B5が利用する場合

図5は、情報提供者X1が提供する情報を、契約者A4が受信して契約者B5に再提供し、契約者B5が再提供された情報を利用する場合の、図1のシステムの動作を示すフローチャートである。以下には、図5を用いて、情報提供者X1から提供される情報を、契約者A4が受信して契約者B5に再提供し、契約者B5のユーザが再

提供された情報を利用する場合について説明する。なお、情報提供者X1から提供された情報は、図3のステップS201～ステップS203と同様にして、情報記録部110aに記録されているものとする。

【0268】契約者A4のユーザが、情報記録部110aに記録された、ある情報を、契約者B5に再提供したい意、および、再提供された情報を契約者Bが利用した場合、契約者Aに課金されるようにするのか、契約者Bに課金されるようにするのかを、ユーザ端末20aに入力すると、ユーザ端末20aは、それらの意を情報サーバ10aに通知する。ユーザ端末20aからの通知を受けると、情報サーバ10aは、付加された情報識別子を参照して、情報記録部110aに記録された情報のうち、ユーザが求める情報を見出す。そして、情報サーバ10aは、その情報が情報提供者X1から提供されたものであることを認識し、その情報をXの復号部102aに入力する。Xの復号部102aは、入力された情報を復号する（ステップS401）。次に、Xの課金部103aは、ユーザ端末20aからの通知に基づいて、契約者A4に課金するか否かを判定する（ステップS402）。

【0269】契約者A4に課金する場合、Xの課金部103aは、上記オフライン端末50aで利用する場合と同様にして、実行権データを作成するとともに、作成した実行権データに応じた利用料金を算定する（ステップS403）。そして、データ記録部112aは、Xの課金部103aが算定して得られた利用料金を記録する（ステップS404）。ただし、この場合、作成された実行権データに含まれる利用可能回数は、契約者A4のユーザが申告した、その情報を契約者B5に利用させる回数であり、記録モードは、契約者B5のユーザ端末20bで利用されることを示す2、課金モードは、契約者A4に課金済みであることを示す1である。また、算定された利用料金は、契約者B5のユーザが、ユーザ端末20bで、その情報を利用可能回数に等しい回数だけ利用した場合の料金である。

【0270】契約者B5に課金する場合には、Xの課金部103aは、実行権データを作成する（ステップS405）。ただし、この場合、作成された実行権データに含まれる利用可能回数は、予め定められた十分大きな値であり、記録モードは、契約者B5のユーザ端末20bで利用されることを示す2、課金モードは、未課金であることを示す2である。

【0271】次に、共通暗号化部111aは、Xの復号部102aが復号して得られた情報を、上記リアルタイムに利用する場合と同様にして、乱数発生部113aが発生した乱数 r で再暗号化する（ステップS406）。そして、情報サーバ10aは、共通暗号化部111aが再暗号化して得られた情報を移動ディスク30aに記録し（ステップS407）、乱数発生部113aが発生し

た乱数 r および X の課金部 103a が作成した実行権データを IC カード 40a に記録する (ステップ S408)。

【0272】 契約者 B5 のユーザは、再暗号化された情報が記録された移動ディスク 30a と乱数 r および実行権データが記録された IC カード 40a とを取得すると、取得した移動ディスク 30a および IC カード 40a を、ユーザ端末 20b に接続し (ステップ S409)、次いで、移動ディスク 30a に記録された情報を利用する意を、ユーザ端末 20b に入力する。

【0273】 ユーザ端末 20b の共通復号部 201b は、最初、IC カード 40a に記録された実行権データに含まれる課金モードが 1 であるか否か、すなわち契約者 A4 に課金済みであるか否かを判定する (ステップ S410)。課金モードが 1 である場合、共通復号部 201b は、実行権データに含まれる記録モードが 2 であるか否か、すなわち、その情報が契約者 B5 のユーザ端末 20b で利用されるべきものであるか否かを、さらに判定する (ステップ S411)。記録モードが 2 である場合、共通復号部 201b は、実行権データに含まれる利用可能回数が 1 以上であるか否かを、さらに判定する (ステップ S412)。

【0274】 利用可能回数が 1 以上である場合、共通復号部 201b は、移動ディスク 30a に記録された、再暗号化された情報を、上記リアルタイムに利用する場合と同様にして、IC カード 40a に記録された乱数 r で復号する (ステップ S413)。次に、ユーザ端末 20b は、実行権データに含まれている利用可能回数を更新し (ステップ S414)、共通復号部 201b が復号して得られた情報を表示する。こうして、契約者 B5 のユーザは、契約者 A4 から再提供された情報を利用することができる (ステップ S415)。

【0275】 ステップ S411 で、記録モードが 2 でない場合、もしくは、ステップ S412 で、利用可能回数が 0 である場合には、共通復号部 201b は、再暗号化された情報を乱数 r で復号する動作を行わず、ユーザ端末 20b がユーザに対して、その情報を利用できない意を通知する (ステップ S416)。

【0276】 ステップ S410 で、課金モードが 1 でない場合、すなわち、未課金である場合には、ユーザ端末 20b は、情報サーバ 10b に、移動ディスク 30a に記録された、再暗号化された情報に付加された課金基準データを通知する。情報サーバ 10b の X の課金部 103b は、通知された課金基準データに基づいて、その情報の利用料金を算定し (ステップ S417)、データ記録部 112b は、 X の課金部 103b が算定して得られた利用料金を記録する (ステップ S418)。その後、ステップ S411 の処理に進む。

【0277】 このように、契約者 A4 に課金する場合、情報サーバ 10a の X の課金部 103a は、情報の利用

度合およびその情報を利用可能な端末を制限するための実行権データを作成し、かつ、作成した実行権データに応じた利用料金を、その情報に付加された課金基準データに基づいて算定する。その情報および作成された実行権データが契約者 B5 に伝達されると、ユーザ端末 20b は、伝達された実行権データが所定の条件を満たす場合に、伝達された情報を表示する。これにより、契約者 A4 が受信した情報を契約者 B5 が利用する場合、利用度合に応じて、契約者 A4 に課金することができる。

10 【0278】 なお、契約者 A4 が受信した情報を契約者 B5 が利用して、契約者 A4 に課金するという提供形態は、情報をプレゼントするという、情報提供の新たな形態である。

【0279】 契約者 B5 に課金する場合には、情報サーバ 10a の X の課金部 103a は、情報を利用できる端末を制限するための実行権データを作成する。その情報および作成された実行権データが契約者 B5 に伝達されると、情報サーバ 10b の X の課金部 103b は、伝達された情報に付加された課金基準データに基づいて、その情報の利用料金を算定する。一方、ユーザ端末 20b は、伝達された実行権データが所定の条件を満たす場合に、伝達された情報を表示する。これにより、契約者 A4 が受信した情報を契約者 B5 が利用する場合、利用度合に応じて、契約者 B5 に課金することができる。

【0280】 以上は、契約者 A4 から契約者 B5 に、移動ディスク 30a および IC カード 40a を介して、それぞれ、情報、データ類を伝達する場合について説明しているが、以下には、CATV 網を介して、情報およびデータ類を伝達する場合について、図 1 および 5 を用いて説明する。本システムの動作が、図 5 に示すものと異なるのは、以下に示す点である。すなわち、ステップ S406 ~ S408 において、契約者 A4 および契約者 B5 はそれぞれ、共有鍵 KAB を保有しており、共通暗号化部 111a は、 X の復号部 102a が復号して得られた情報を、乱数発生部 113a が発生した乱数 r で再暗号化し、さらに、この乱数 r および X の課金部 103a が作成した実行権データを、共有鍵 KAB で暗号化する。そして、情報サーバ 10a は、共通暗号化部 111a が再暗号化して得られた情報ならびに暗号化して得られた乱数および実行権データを、CATV 網を通じて、契約者 B5 に送信する。

【0281】 また、ステップ S409 において、ユーザ端末 20b が、CATV 網を通じて送信された、再暗号化された情報ならびに暗号化された乱数および実行権データを受信すると、共通復号部 201b は、暗号化された乱数および実行権データを、共有鍵 KAB で復号する。

【0282】 このように、CATV 網のような、伝送速度が比較的大きな伝送路を通じて、情報、乱数および実行権データを伝送する場合には、情報を乱数で再暗号化

し、さらに、乱数および実行権データを共有鍵KABで暗号化することにより、契約者A4から契約者B5に、安全に情報を伝達できる。

【0283】なお、共有鍵KABで乱数および実行権データを暗号化する代わりに、公開暗号方式で暗号化することもできる。また、CATV網に代えて、B-ISDNを通じて、契約者Aから契約者Bに、再暗号化された情報ならびに暗号化された乱数および実行権データを伝送してもよい。

【0284】次に、契約者A4から契約者B5に、移動ディスク30aを介して情報を、通信回線を介してデータ類を、それぞれ伝達する場合について、図1および5を用いて説明する。本システムの動作が、図5に示すものと異なるのは、以下に示す点である。すなわち、ステップS406～S408において、契約者A4および契約者B5はそれぞれ、共有鍵KABを保有しており、共通暗号化部111aは、Xの復号部102aが復号して得られた情報を、乱数発生部113aが発生した乱数rで再暗号化し、さらに、この乱数rおよびXの課金部103aが作成した実行権データを、共有鍵KABで暗号化する。そして、情報サーバ10aは、共通暗号化部111aが再暗号化して得られた情報を、移動ディスク30aに記録し、共通暗号化部111aが暗号化して得られた乱数および実行権データを、通信回線を通じて、契約者B5に送信する。

【0285】また、ステップS409において、契約者B5のユーザは、再暗号化された情報が記録された移動ディスク30aを取得すると、取得した移動ディスク30aを、ユーザ端末20bに接続する。また、ユーザ端末20bが、通信回線を通じて送信された、暗号化された乱数および実行権データを受信すると、共通復号部201bは、暗号化された乱数および実行権データを、共有鍵KABで復号する。

【0286】このように、乱数および実行権データを、通信回線のような、伝送速度が比較的小さい伝送路を通じて伝送し、情報を、移動ディスク30aに記録して移動させる場合には、情報を乱数で再暗号化し、さらに、乱数および実行権データを共有鍵KABで暗号化することにより、契約者A4から契約者B5に、安全に情報を伝達できる。なお、共有鍵KABで乱数および実行権データを暗号化する代わりに、公開暗号方式で暗号化することもできる。

【0287】なお、本実施形態では、実行権データに利用可能回数が含まれるとしたが、利用可能期限が含まれるとしてもよい。

【0288】また、本実施形態では、ユーザがオフライン端末50aで情報を利用する場合、Xの課金部103aは、実行権データを作成すると同時に、作成した実行権に応じた利用料金を算定しているが、オフライン端末50aでの利用度合をICカード40aに記録してお

き、利用後に、ユーザがICカード40aを情報サーバ10aに接続して、その際、Xの課金部103aが利用料金を算定してもよい。

【0289】また、本実施形態では、契約者単位で課金しているが、利用料金を端末毎に記録することにより、ユーザ単位で課金することもできる。

【0290】また、ユーザにパスワードを発行し、ユーザが端末を利用する際に、認証を行うようにすることで、不正使用に対する安全性を、より高めることができる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係る情報提供システムの構成を示すブロック図である。

【図2】情報提供者X1が提供する情報を、契約者Aが受信して、リアルタイムに利用する場合の、図1のシステムの動作を示すフローチャートである。

【図3】情報提供者X1が提供する情報を、契約者A4が受信して記録し、記録した情報を利用する場合の、図1のシステムの動作を示すフローチャートである。

【図4】情報提供者X1が提供する情報を、契約者A4が受信して、オフライン端末50aで利用する場合の、図1のシステムの動作を示すフローチャートである。

【図5】情報提供者X1が提供する情報を、契約者A4が受信して契約者B5に再提供し、契約者B5が再提供された情報を利用する場合の、図1のシステムの動作を示すフローチャートである。

【図6】従来の映像情報伝送装置の構成を示すブロック図である。

【符号の説明】

- | | |
|-----------|---------|
| 1 | 情報提供者X |
| 2 | 情報提供者Y |
| 3 | 情報提供者Z |
| 4 | 契約者A |
| 5 | 契約者B |
| 10a、10b | 情報サーバ |
| 20a、20b | ユーザ端末 |
| 30a、30b | 移動ディスク |
| 40a、40b | ICカード |
| 50a | オフライン端末 |
| 101a、101b | Xの受信部 |
| 102a、102b | Xの復号部 |
| 103a、103b | Xの課金部 |
| 104a、104b | Yの受信部 |
| 105a、105b | Yの復号部 |
| 106a、106b | Yの課金部 |
| 107a、107b | Zの受信部 |
| 108a、108b | Zの復号部 |
| 109a、109b | Zの課金部 |
| 110a、110b | 情報記録部 |
| 111a、111b | 共通暗号化部 |

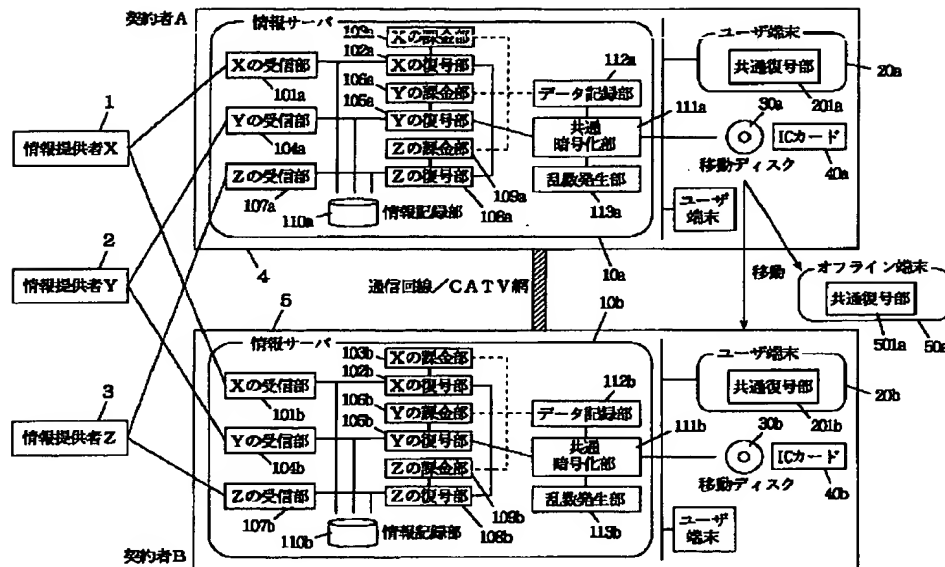
112a、112b データ記録部

* 201a、201b、501a 共通復号部

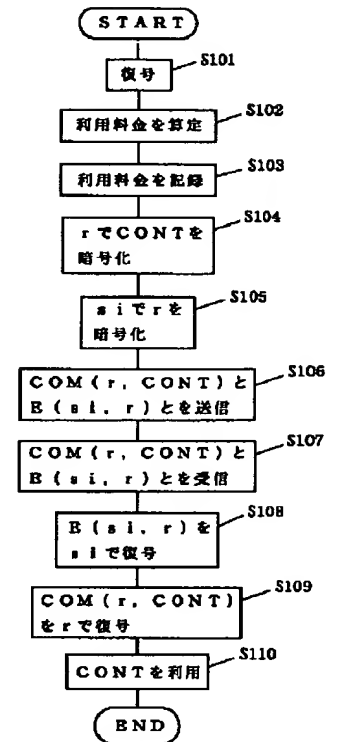
113a、113b 乱数発生部

*

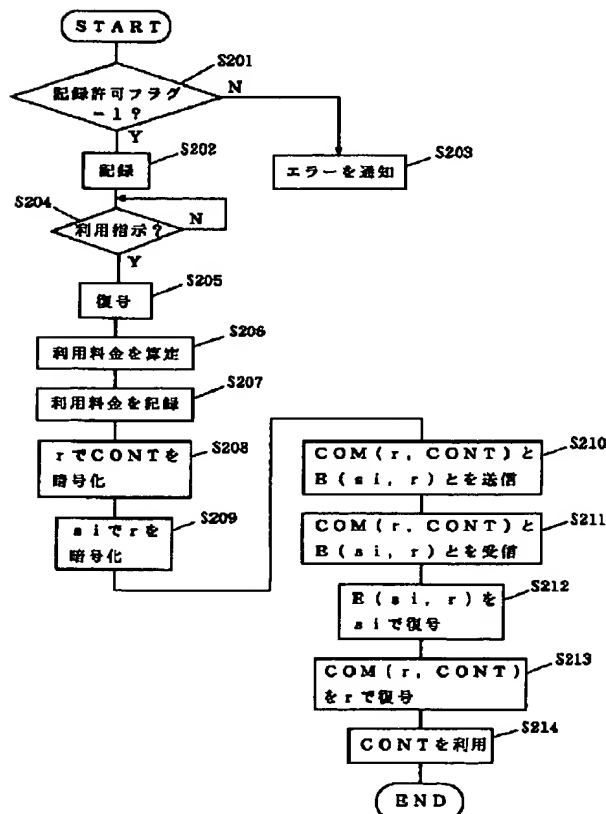
【図1】



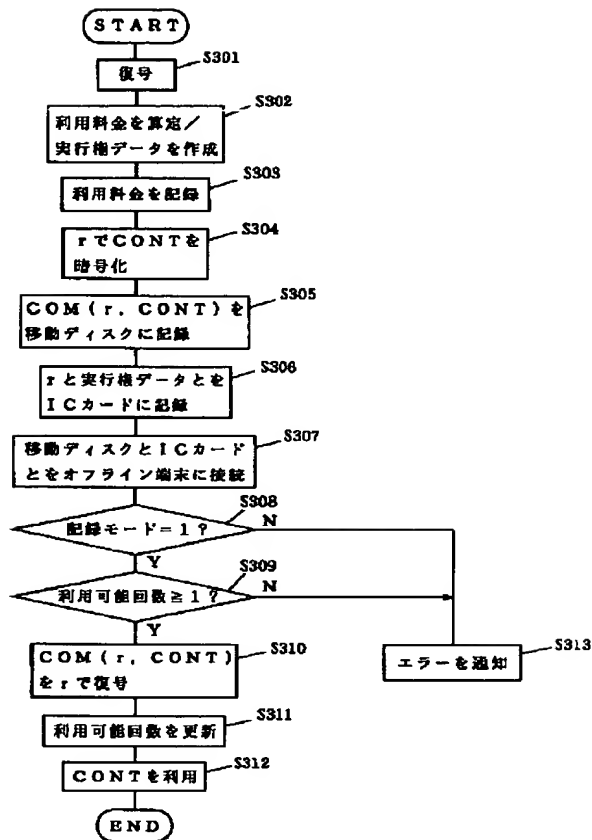
【図2】



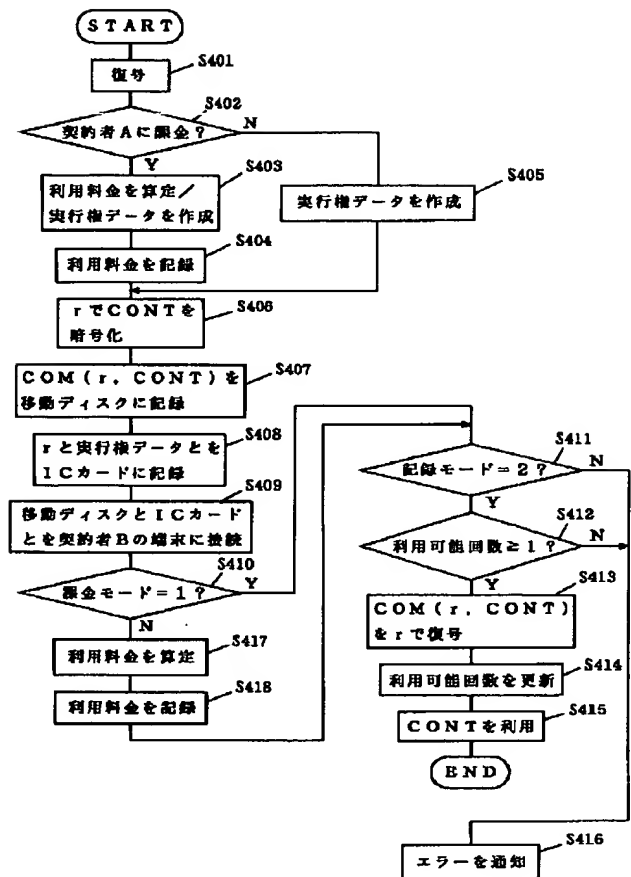
【図3】



【図4】



【図5】



【図6】

